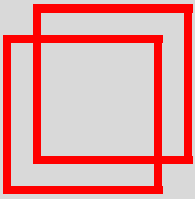

Math-Net.Ru
Общероссийский математический портал

А. С. Кузьмин, А. А. Нечаев, В. А. Шишкин, Параметры (гипер-) бент-функций над полем из 2^l элементов,
Тр. по дискр. матем., 2008, том 11, выпуск 1, 47–59

https://www.mathnet.ru/tdm179

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.9.172
22 мая 2025 г., 00:32:49

Труды по дискретной математике
Том 11, с. 47–59
М.: ФИЗМАТЛИТ, 2008

ПАРАМЕТРЫ (ГИПЕР-) БЕНТ-ФУНКЦИЙ НАД ПОЛЕМ ИЗ 2^l ЭЛЕМЕНТОВ

А. С. КУЗЬМИН, А. А. НЕЧАЕВ, В. А. ШИШКИН

Продолжены исследования параметров бент- и гипербент-функций над полем P из $q = 2^l$, $l > 1$, элементов, начатые в [1, 3, 8, 9]. Показано, что наиболее точное обобщение результатов о параметрах таких функций со случая $l = 1$ (см. [7]) на случай $l > 1$ получается, если в качестве основного исследуемого параметра вместо степени нелинейности функции рассматривать ее двоичный индекс нелинейности (в случае $l = 1$ эти параметры совпадают).

§ 1. ВВЕДЕНИЕ, ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Здесь продолжаются исследования, начатые в [1, 8]. Пусть $P = \mathbf{F}_q$ — конечное поле мощности $q = 2^l$, $l \geqslant 1$. Изучаются возможности приближения произвольной функции

$$f\colon P^n \to P, \quad f = f(\mathbf{x}) = f(x_1, \ldots, x_n) \tag{1.1}$$

функциями из некоторого ограниченного класса $\mathcal{A}$ функций (1.1). Вместо $f(\mathbf{x})$ удобно рассматривать функции $F\colon Q \to P$, где $Q = \mathbf{F}_{q^n}$ — расширение степени n поля P. Зафиксируем базис $\alpha_1, \ldots, \alpha_n$ пространства Q_P. Тогда функция $f(x_1, \ldots, x_n)$ от набора независимых свободных переменных $\mathbf{x} = (x_1, \ldots, x_n)$ на P отождествляется с функцией $F(x)$ от свободного переменного x на Q вида $x = \alpha_1 x_1 + \ldots + \alpha_n x_n$:

$$F(x) = f(x_1, \ldots, x_n). \tag{1.2}$$

Функции $F(x)$ и $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ называются соответствующими друг другу. В качестве класса $\mathcal{A}$ приближающих функций рассматривается один из следующих двух классов.

i) Класс $\mathcal{H} = \mathrm{Hom}_{\mathbf{Z}}(Q, P)$ всех гомоморфизмов групп $h : (Q, +) \to (P, +)$, каждый из которых при фиксированном базисе $\varepsilon_1, \ldots, \varepsilon_l$ пространства P_S, где

© А. С. Кузьмин, А. А. Нечаев, В. А. Шишкин, 2008

$S = \mathbf{F}_2$ — простое подполе поля P, однозначно представляется в виде

$$h(x) = \sum_{j=1}^{l} \varepsilon_j \cdot \mathrm{tr}_S^Q(\beta_j x), \quad \text{где } \beta_1, \ldots, \beta_l \in Q, \tag{1.3}$$

$\mathrm{tr}_S^Q(x) = x + x^p + \ldots + x^{p^{nl-1}}$ — след из поля Q в поле S; а также — в виде

$$h(x) = \mathrm{tr}_P^Q\left(\sum_{i=0}^{l-1} h_i x^{p^i}\right), \quad \text{где } h_0, \ldots, h_{l-1} \in Q. \tag{1.4}$$

В случае $l = 1$ класс $\mathcal{H}$ превращается в множество всех линейных функций.

ii) Класс $\mathcal{M} = \mathcal{M}(Q, P)$ всех функций вида

$$g(x) = h(x^k), \quad k \in \mathbf{Z}_{q^n-1}^*, \quad h \in \mathcal{H}, \tag{1.5}$$

называемых собственными обобщенными мономиальными функциями из Q в P. Пусть $N_a(F)$ — число решений в поле Q уравнения $F(x) = a \in P$. В качестве основного параметра, характеризующего степень близости функции F и приближающей ее функции $A : Q \to P$ мы используем функцию согласие:

$$\nabla(F, A) = \left(\frac{q}{q-1} \sum_{a \in P} \left(\frac{N_a(F-A)}{q^n} - \frac{1}{q}\right)^2\right)^{1/2}. \tag{1.6}$$

Возможности аппроксимации функции $F\colon Q \to P$ функциями из класса $\mathcal{A}$ и возможности класса $\mathcal{A}$ аппроксимировать произвольную функцию из P^Q характеризуют соответственно параметры

$$\nabla(F, \mathcal{A}) = \max\{\nabla(F, h)\colon h \in \mathcal{A}\} \quad \text{и} \quad \nabla\mathcal{A} = \min\{\nabla(F, \mathcal{A})\colon F \in P^Q\}.$$

Для класса $\mathcal{A} = \mathcal{H}$ справедливо неравенство: $\nabla\mathcal{H} \geqslant \dfrac{1}{\sqrt{|Q|}} = q^{-\lambda}$ [1, 3], где $\lambda = \dfrac{n}{2} \in \mathbf{Q}$. Как и для $q = 2$, назовем $F \in P^Q$ и соответствующую функцию $f \in P^{P^n}$ бент-функцией, если

$$\nabla(F, \mathcal{H}) = q^{-\lambda},$$

т. е. если функция F одинаково плохо приближается всеми гомоморфизмами $h\colon Q \to P$. Существование бент-функций при $l > 1$ было доказано в [1].

Для любой функции $f\colon P^n \to P$ существует единственное полиномиальное представление, в котором каждый моном содержит переменные в степенях, не превосходящих $q - 1$:

$$f(x_1, \ldots, x_n) = \sum_{k_1, \ldots, k_n \in \{0, \ldots, q-1\}} a_{k_1 \ldots k_n} x_1^{k_1} \ldots x_n^{k_n}. \tag{1.7}$$

Это представление называется приведенным полиномиальным представлением, и степень полинома в его правой части называется степенью (нелинейности) функции f и обозначается символом $\deg f$.

Из результатов В. А. Елисеева и О. П. Степченкова (1962, устное сообщение), а также из [4, 5] вытекает следующая теорема.

Теорема 1.1. *Пусть $q = 2$, т. е. $l = 1$. Тогда равенство $\nabla\mathcal{H} = 2^{-\lambda}$ выполняется (т. е. существуют бент-функции), если и только если $n = 2\lambda$ — четное число, причем в этом случае любая бент-функция f удовлетворяет неравенству $\deg f \leqslant \lambda$.*

В [8] был получен следующий результат.

Теорема 1.2. *Пусть $q = 2^l$ и $f(\mathbf{x}) \in P[x_1, \ldots, x_n]$ — бент-функция, тогда*

а) *ln — четное число;*

б) *Если $n = 2\lambda > 2$, где $\lambda \in \mathbf{Q}$, то для любого $a \in P$*

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

где n_a — нечетное число из интервала $\{-(q-1), \ldots, q-1\}$;

в) *при условиях* (б) $\deg f(\mathbf{x}) \leqslant n(q-1) - \lambda$.

Формально последняя оценка является точным обобщением оценки степени нелинейности бент-функции при $l = 1$. Однако при $l > 1$ она оказывается весьма грубой, поскольку недостаточно точно ограничивает множество функций, являющихся «кандидатами» в бент-функции.

Результаты данной работы показывают, что при $l > 1$ более эффективные ограничения на класс бент-функций можно получить, изучая двоичный индекс нелинейности функции, определяемый следующим образом.

Для $q \in \mathbf{N} \setminus \{1\}$ и произвольного числа $m \in \mathbf{N}_0$ с q-ичным разложением $m = m_0 + qm_1 + \ldots$, $m_i \in \{0, \ldots, q-1\}$, определим q-ичную норму равенством $\|m\|_q = m_0 + m_1 + \ldots$ Назовем двоичным индексом нелинейности функции (1.7) число

$$\operatorname{ind}_2 f = \max\{\|k_1\|_2 + \ldots + \|k_n\|_2 \colon (k_1, \ldots, k_n) \in \{0, \ldots, q-1\}^n,\ a_{k_1 \ldots k_n} \neq 0\}.$$

Заметим, что в случае $l = 1$ справедливы соотношения $\operatorname{ind}_2 f = \deg f \leqslant n$, а при $l > 1$ имеют место неравенства $\operatorname{ind}_2 f \leqslant nl$, $\deg f \leqslant n(2^l - 1)$. Наша первая цель: оценить параметр $\operatorname{ind}_2 f$ для бент-функций.

Полученные результаты основаны на изучении приведенного представления функции F, соответствующей f. Для любого $c \in \mathbf{Z}$ положим

$$\rho(c) = \rho_{q^n-1}(c) \in \{1, \ldots, q^n - 1\}, \quad \rho(c) \equiv c \pmod{q^n - 1}.$$

Для $k \in \{1, \ldots, q^n - 1\}$ положим

$$\mu(k) = \mu_q^{q^n}(k) = \min\{k, \rho(kq), \ldots, \rho(kq^{n-1})\}.$$

Определим множество $M = M_q^{q^n}$ как совокупность всех различных чисел $\mu(k)$ для $k \in \{1, \ldots, q^n - 1\}$. Зафиксируем примитивный элемент $\theta \in Q$. Для каждого $k \in M$ определим $Q_k = P(\theta^k)$, где $P(\theta^k)$ — подполе поля Q, полученное расширением поля P элементом θ^k, и зафиксируем элемент $\xi_k \in Q$ так, что $\mathrm{tr}_{Q_k}^{Q}(\xi_k) = e$.

Теорема 1.3 [8]. *Для любой сохраняющей 0 функции $F \in P^Q$ существует единственное представление в виде*

$$F(x) = \mathrm{tr}_P^Q(\Phi(x)), \quad \Phi(x) = \sum_{k \in M} c_k \cdot \xi_k \cdot x^k, \quad c_k \in Q_k, \ k \in M = M_q^{q^n}. \quad (1.8)$$

Представление (1.8) называется приведенным представлением для $F(x)$, а многочлен $\Phi(x)$ — редуцированным многочленом, представляющим $F(x)$. Определим носитель $S(\Phi)$ представляющего многочлена Φ равенством $S(\Phi) = \{k \in M : c_k \neq 0\}$. При условии (1.8) определим двоичный индекс нелинейности $\mathrm{ind}_2 \Phi(x)$ многочлена $\Phi(x)$ равенством

$$\mathrm{ind}_2 \Phi(x) = \max\{\|k\|_2 : k \in S(\Phi)\}.$$

Аналогично определяем двоичный индекс нелинейности $\mathrm{ind}_2 F(x)$ многочлена $F(x)$.

Ниже доказаны следующие результаты.

Теорема 1. *Двоичные индексы нелинейности многочлена $f(\mathbf{x})$ и соответствующего ему многочлена $F(x)$, имеющего приведенное представление* (1.8), *удовлетворяют равенствам* $\mathrm{ind}_2 f = \mathrm{ind}_2 F = \mathrm{ind}_2 \Phi$.

Теорема 2. *Если $f(x_1, \ldots, x_n)$ — бент-функция, то*

$$\mathrm{ind}_2 f \leqslant \frac{nl}{2}. \quad (1.9)$$

Из полученного ограничения сверху на индекс нелинейности 2^l-значной бент-функции следует также ограничение сверху на ее степень нелинейности, более сильное, чем в теореме 1.2.

Теорема 3. *Если $f(x_1, \ldots, x_n) \in P^{P^n}$ и $\mathrm{ind}_2 f \leqslant \frac{nl}{2}$, в частности, если f — бент-функция, то* $\deg f \leqslant n(q - \sqrt{q})$, *а если l нечетно, то* $\deg f \leqslant n\left(q - \frac{3}{2\sqrt{2}}\sqrt{q}\right)$.

Вторая часть работы посвящена исследованию возможностей аппроксимации произвольной функции F функциями из класса $\mathcal{M} = \mathcal{M}(Q, P)$ всех собственных обобщенных мономиальных функций из Q в P:

$$g(x) = h(x^k), \quad k \in \mathbf{Z}_{q^n-1}^*, \quad h \in \mathcal{H} = \mathrm{Hom}(Q, P).$$

Заметим, что $\mathcal{H} \subset \mathcal{M}$, и потому $\nabla\mathcal{M} \geqslant \frac{1}{\sqrt{|Q|}} = q^{-\lambda}$.

Назовем функцию $F \in P^Q$ и соответствующую функцию $f \in P^{P^n}$ гипер-бент-функциями (ГБ-функциями), если $\nabla(F, \mathcal{M}) = q^{-\lambda}$, т. е. если функция F одинаково плохо приближается всеми собственными мономиальными функциями $g(x)$.

Существование ГБ-функций доказывает следующий результат, обобщающий результат работы [6], полученный для $q = 2$. Пусть $q = 2^l$, $n = 2\lambda$, $\lambda \in \mathbf{N}$. Имеем разложение: $Q^* = R^* \dot{\times} V$, где $R = \mathbf{F}_{q^\lambda}$, V — циклическая группа порядка $q^\lambda + 1$. Для любой функции $F\colon Q \to P$ обозначим через $N_a(F|V)$ число решений уравнения $F(x) = a$ в множестве V.

Теорема 1.4 [8]. *Пусть функция $H\colon V \to P$ такова, что для некоторого $d \in P$*

$$N_d(H \mid V) = q^{\lambda-1} + 1, \quad N_a(H \mid V) = q^{\lambda-1}, \quad \text{если } a \in P \setminus \{d\}. \tag{1.10}$$

Тогда функция $F\colon Q \to P$, определяемая условиями

$$F(0) = d, \quad F(x) = H(x^{q^\lambda - 1}) \quad \text{для } x \neq 0, \tag{1.11}$$

есть гипер-бент-функция.

Положим

$$B(\lambda) = B_q^{q^n}(\lambda) = \left\{k \in M\colon \lambda \leqslant \|\rho(k\sigma)\|_q \leqslant (q-1)n - \lambda \ \ \forall \sigma \in \mathbf{Z}_{q^n-1}^*\right\}.$$

Теорема 1.5 [8]. *Пусть $F(x)$ есть ГБ-функция, сохраняющая* 0. *Тогда*

$$S(\Phi) \subseteq B(\lambda); \tag{1.12}$$

$$\lambda \leqslant \deg f(\mathbf{x}) \leqslant (q-1)n - \lambda. \tag{1.13}$$

Следствие 1.6 [8]. *В условиях теоремы* 1.5 *множество $S(\Phi)$ не содержит чисел, взаимно простых с $q^n - 1$.*

Введем следующее обозначение:

$$M_q^{q^n}(s) = \left\{k \in M_q^{q^n}\colon \|\rho(k\sigma)\|_2 = s \ \ \forall \sigma \in \mathbf{Z}_{q^n-1}^*\right\}. \tag{1.14}$$

В случае $q = 2$, $n = 2\lambda$, $\lambda \in \mathbf{N}$ множество $B(\lambda)$ совпадает с $M_2^{2^n}(\lambda)$. Таким образом, согласно теореме 1.5, при условии $q = 2$ ГБ-функция F удовлетворяет условию

$$S(\Phi) \subseteq M_2^{2^n}(\lambda). \tag{1.15}$$

Это утверждение теоремы 2 работы [7]. Таким образом, теорему 1.5 можно рассматривать как обобщение указанной теоремы 2. Однако следующий

результат показывает, что можно рассчитывать на гораздо более точное обобщение.

ТЕОРЕМА 1.7 [8]. *Пусть* $q = 2^l \geqslant 2$, $n = 2\lambda$, $\lambda \in \mathbf{N}$ *и* $F\colon Q \to P$ — *ГБ-функция из теоремы* 1.4, *сохраняющая* 0, *т. е. такая, что* $d = 0$. *Тогда редуцированный многочлен* $\Phi(x)$, *представляющий* $F(x)$, *удовлетворяет условию*

$$S(\Phi) \subseteq M_q^{q^n}(l\lambda). \tag{1.16}$$

Здесь получено желаемое уточнение, что позволяет также найти более жесткие ограничения на степень и двоичный индекс нелинейности ГБ-функции.

ТЕОРЕМА 4. *Пусть* $q = 2^l$, $n = 2\lambda$, $\lambda \in \mathbf{N}$, *и* $F\colon Q \to P$ *есть ГБ-функция, сохраняющая* 0. *Тогда*

а) *при условии* (1.8) *выполняется включение* (1.16), *т. е. многочлен* F *однозначно представляется в виде*

$$F(x) = \operatorname{tr}_P^Q(\Phi(x)), \quad \Phi(x) = \sum_{k \in M_q^{q^n}(l\lambda)} c_k \cdot \xi_k \cdot x^k, \quad c_k \in Q_k,\ k \in M_q^{q^n}(l\lambda); \tag{1.17}$$

б) *если все числа из множества* $M_q^{q^n}(l\lambda)$ *делятся на* $q^\lambda - 1$, *то любая ГБ-функция* $F\colon Q \to P$ *имеет вид, описанный в теореме* 1.4;

в) *функция* $f(\mathbf{x})$, *соответствующая* F, *удовлетворяет условию*

$$\operatorname{ind}_2 f(\mathbf{x}) = \operatorname{ind}_2 F(x) = \operatorname{ind}_2 \Phi(x) = \lambda l = \frac{nl}{2}. \tag{1.18}$$

В связи с результатом теоремы 1.5 представляет интерес задача описания множества $M_q^{q^n}(l\lambda)$ или оценки его мощности. Следующее предложение представляет собой обобщение на случай $q = 2^l > 2$ свойств такого множества, полученных в работе [7] для $q = 2$.

ТЕОРЕМА 5. *Пусть* $q = 2^l$, $n = 2\lambda$, $\lambda \in \mathbf{N}$. *Тогда*

а) *для любого натурального делителя* s *числа* λ *справедливо включение*

$$\frac{q^n - 1}{q^s + 1} \in M_q^{q^n}(l\lambda), \tag{1.19}$$

в частности,

$$\frac{q^n - 1}{q + 1} \in M_q^{q^n}(l\lambda), \quad q^\lambda - 1 \in M_q^{q^n}(l\lambda);$$

б) *для любого* $a \in \{1, \ldots, q^\lambda\}$ *выполняется включение* $\mu((q^\lambda - 1)a) \in$ $\in M_q^{q^n}(l\lambda)$;

в) *если* $t \in \mathbf{N} \setminus \{1\}$, $m = 1 + q^n + \ldots + q^{(t-1)n}$, *то*

$$mM_q^{q^n}(l\lambda) \subseteq M_q^{q^{tn}}(tl\lambda). \tag{1.20}$$

Будем называть элементы $k, m \in M_q^{q^n}(l\lambda)$ ассоциированными и писать $k \sim m$, если $m = \rho(k\sigma)$ для некоторого $\sigma \in \mathbf{Z}_{q^n-1}^*$. Отношение $\sim$ есть отношение эквивалентности на $M_q^{q^n}(l\lambda)$. Пусть $[k]$ — класс чисел из $M_q^{q^n}(l\lambda)$, ассоциированных с k.

Теорема 6. *Пусть* $q = 2^l$, $n = 2\lambda$, $\lambda \in \mathbf{N}$. *Если* $k \in M_q^{q^n}(l\lambda)$ *и* $d = \text{НОД}(k, q^n - 1)$, *то* $d \in [k]$ *и* d *— единственный делитель числа* $q^n - 1$, *принадлежащий классу* $[k]$. *Пусть* $D_q^{q^n}(l\lambda)$ *— множество чисел* $d \in M_q^{q^n}(l\lambda)$, *делящих* $q^n - 1$. *Тогда*

$$M_q^{q^n}(l\lambda) = \bigcup_{d \in D_q^{q^n}(l\lambda)} [d].$$

§ 2. ДВОИЧНЫЙ ИНДЕКС НЕЛИНЕЙНОСТИ БЕНТ-ФУНКЦИИ

Доказательство теоремы 1. Из (1.8) следует, что многочлен $F(x)$ есть сумма мономов вида $c_k^{q^i} x^{kq^i}$, где $k \in M$, $i \in \{0, \ldots, t_k - 1\}$, t_k — порядок элемента q в мультипликативной группе кольца вычетов по модулю $\dfrac{q^n - 1}{\text{НОД}(q^n - 1, k)}$. Очевидно, $\text{ind}_2(c_k^{q^i} x^{kq^i}) = \text{ind}_2(c_k x^k)$, откуда в силу определений следует равенство $\text{ind}_2 F = \text{ind}_2 \Phi$.

При обозначениях (1.2) функция f получается из F заменой каждого монома $G(x) = bx^m$ на многочлен $g(x_1, \ldots, x_n) = b\Big(\sum_{j \in \{1,\ldots,n\}} x_j \alpha_j\Big)^m$. При этом, если $\text{ind}_2 G = t$, то $m = 2^{i_1} + \ldots + 2^{i_t}$ и

$$g(x_1, \ldots, x_n) = b\Bigg(\sum_{j \in \{1,\ldots,n\}} (x_j \alpha_j)^{2^{i_1}}\Bigg) \cdot \ldots \cdot \Bigg(\sum_{j \in \{1,\ldots,n\}} (x_j \alpha_j)^{2^{i_t}}\Bigg).$$

Отсюда легко видеть, что $\text{ind}_2 g \leqslant t$ и потому $\text{ind}_2 f \leqslant \text{ind}_2 F = t$.

Докажем обратное неравенство. Пусть $\beta_1, \ldots, \beta_n$ — базис пространства Q_P, двойственный исходному базису $\alpha_1, \ldots, \alpha_n$, т. е. базис, удовлетворяющий условию

$$\text{tr}_P^Q(\alpha_i \cdot \beta_j) = \delta_{ij} e, \quad i, j \in \{1, \ldots, n\}.$$

Тогда из (1.2) следуют равенства

$$x_i = \text{tr}_P^Q(\beta_i x), \ i \in \{1, \ldots, n\}, \quad F(x) = f(\text{tr}_P^Q(\beta_1 x), \ldots, \text{tr}_P^Q(\beta_n x)).$$

Таким образом, многочлен F получается указанной заменой переменных в каждом мономе $g(\mathbf{x}) = dx_1^{k_1} \dots x_n^{k_n}$ многочлена f. Пусть $\operatorname{ind}_2 g = t$. Тогда $g(\mathbf{x})$ можно представить в виде

$$g(\mathbf{x}) = dx_{i_1}^{2^{r_1}} \dots x_{i_t}^{2^{r_t}},$$

где $i_1, \dots, i_t$ — не обязательно различные индексы и $r_1, \dots, r_t \in \{0, \dots, l-1\}$. После замены переменных моном g превращается в многочлен

$$G(x) = d\left(\operatorname{tr}_P^Q(\beta_{i_1}x)^{2^{r_1}}\right) \cdot \dots \cdot \left(\operatorname{tr}_P^Q(\beta_{i_t}x)^{2^{r_t}}\right) =$$

$$= d\left(\sum_{s\in\{0,\dots,n-1\}} (\beta_{i_1}x)^{2^{r_1+sl}}\right) \cdot \dots \cdot \left(\sum_{s\in\{0,\dots,n-1\}} (\beta_{i_t}x)^{2^{r_t+sl}}\right).$$

Из последнего равенства очевидно, что $\operatorname{ind}_2 G(x) \leqslant t = \operatorname{ind}_2 g(\mathbf{x})$. Отсюда $\operatorname{ind}_2 F(x) \leqslant \operatorname{ind}_2 f(\mathbf{x})$.

Таким образом, $\operatorname{ind}_2 F(x) = \operatorname{ind}_2 f(\mathbf{x})$.

Теорема 3(1) работы [1] дает следующее определяющее свойство бент-функций (здесь мы формулируем его в иной, но эквивалентной форме).

Теорема 2.1. *Функция $F\colon Q \to P$ является бент-функцией тогда и только тогда, когда для любого элемента $b \in P^*$ функция $\operatorname{tr}_S^P(bF(x)) \in S^Q$ является бент-функцией.*

Доказательство теоремы 2. Пусть $\gamma_1, \dots, \gamma_l$ — базис пространства P_S, двойственный исходному базису $\varepsilon_1, \dots, \varepsilon_l$ этого пространства, т. е. базис, удовлетворяющий условию

$$\operatorname{tr}_P^Q(\varepsilon_i \cdot \gamma_j) = \delta_{ij}e.$$

Для каждого $x \in Q$ имеет место разложение

$$F(x) = \sum_{j=1}^{l} \gamma_j F_j(x), \tag{2.1}$$

где $F_j(x) \in S^Q$. При этом

$$F_j(x) = \operatorname{tr}_S^P(\varepsilon_j F(x)), \quad j \in \{1, \dots, l\}. \tag{2.2}$$

Действительно,

$$\operatorname{tr}_S^P(\varepsilon_j F(x)) = \operatorname{tr}_S^P\left(\varepsilon_j\left(\sum_{i=1}^{l} \gamma_i F_i(x)\right)\right) = \sum_{i=1}^{l} \operatorname{tr}_S^P(\varepsilon_j\gamma_i F_i(x)) =$$

$$= \sum_{j=1}^{l} F_i(x) \operatorname{tr}_S^P(\varepsilon_j\gamma_i) = F_j(x).$$

Так как по условию теоремы $F(x)$ есть бент-функция, то из (2.2) по теореме 2.1 следует, что каждая из функций $F_j(x) = \mathrm{tr}_S^P(\varepsilon_j F(x))$ есть бент-функция на Q со значениями в $S = \mathbf{F}_2$ и ей соответствует булева бент-функция $f_j(\mathbf{y})$ от $nl = [Q : S]$ переменных $\mathbf{y} = (y_1, \ldots, y_{nl})$. Так как $\mathrm{ind}_2 f_j = \deg f_j$, то $\mathrm{ind}_2 f_j \leqslant \dfrac{nl}{2}$ по теореме 1.1, и $\mathrm{ind}_2 F_j \leqslant \dfrac{nl}{2}$ по теореме 1. Теперь из (2.1) следует неравенство $\mathrm{ind}_2 F \leqslant \dfrac{nl}{2}$.

Доказательство теоремы 3. Пусть моном $x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ входит в разложение функции f в виде многочлена из $P[x_1, \ldots, x_n]$ с ненулевым коэффициентом. Пусть $k = k_1 + k_2 q + \ldots + k_n q^{n-1}$, тогда по условию теоремы $\|k\|_2 \leqslant \dfrac{nl}{2}$.

Пусть $k = \alpha_0 + \alpha_1 q + \ldots + \alpha_{n-1} q^{n-1}$, $k = a_0 + a_1 2 + \ldots + a_{nl-1} 2^{nl-1}$ — соответственно q-ичное и двоичное разложения числа k. При этом, ввиду единственности двоичного разложения числа k, необходимо выполняется: $\alpha_j = a_{jl} + a_{jl+1} 2 + \ldots + a_{jl+l-1} 2^{l-1}$ для всех $j \in \{0, \ldots, n-1\}$. Отметим, что при условии $\|k\|_2 \leqslant \dfrac{nl}{2}$ среди чисел $a_0, \ldots, a_{nl-1}$ не более $\dfrac{nl}{2}$ единиц, при этом максимум числа $\|k\|_q$ имеет место, когда эти единицы сосредоточены в старших разрядах чисел α_j, $j \in \{0, \ldots, n-1\}$.

а) Пусть l четно. Тогда максимум числа $\|k\|_q$ достигается, когда единицы среди чисел $a_0, \ldots, a_{nl-1}$ сосредоточены в разрядах от $(l-1)$-го по $\dfrac{l}{2}$-й, другими словами, когда $a_{jl+i} = 0$ при $j \in \{0, \ldots, n-1\}$, $i \in \left\{0, \ldots, \dfrac{l}{2} - 1\right\}$. Тогда $\|\alpha_j\|_q \leqslant 2^{l-1} + \ldots + 2^{\frac{l}{2}}$, $j \in \{0, \ldots, n-1\}$, и $\|k\|_q \leqslant n(2^{l-1} + \ldots + 2^{\frac{l}{2}})$. Остается заметить, что

$$2^{l-1} + \ldots + 2^{\frac{l}{2}} = (2^{l-1} + \ldots + 2^{\frac{l}{2}} + 2^{\frac{l}{2}-1} + \ldots + 1) - (2^{\frac{l}{2}-1} + \ldots + 1) =$$

$$= (2^l - 1) - (2^{\frac{l}{2}} - 1) = q - \sqrt{q}.$$

б) Пусть теперь l нечетно. При $l = 1$ выполняется равенство $\deg f = \deg_q f$ и теорема для этого случая тривиальна. Пусть $l > 1$. Тогда максимум числа $\|k\|_q$ достигается, когда единицы среди чисел $a_0, \ldots, a_{nl-1}$ сосредоточены в разрядах от $(l-1)$-го по $\dfrac{l+1}{2}$-й и ровно в половине разряда $\dfrac{l-1}{2}$, другими словами, когда $a_{jl+i} = 0$ при $j \in \{0, \ldots, n-1\}$, $i \in \left\{0, \ldots, \dfrac{l-1}{2} - 1\right\}$ и не

менее половины чисел $a_{jl+\frac{l-1}{2}}$, $j \in \{0, \ldots, n-1\}$, равны нулю. Тогда

$$\|k\|_q \leqslant n(2^{l-1} + \ldots + 2^{\frac{l+1}{2}}) + \frac{n}{2} \cdot 2^{\frac{l-1}{2}} =$$

$$= n(q-1) - n(2^{\frac{l+1}{2}} - 1) + n2^{\frac{l-3}{2}} = n\left(q - \frac{3}{2\sqrt{2}}\sqrt{q}\right).$$

Остается заметить, что если $l > 1$, то $n\left(q - \frac{3}{2\sqrt{2}}\sqrt{q}\right) < n(q - \sqrt{q})$.

Примеры 2^l-значных бент-функций, построенные в работе [8], показывают, что оценка индекса нелинейности (1.9) достижима при любом $l \in \mathbf{N}$.

§ 3. СВОЙСТВА ПРИВЕДЕННОГО ПРЕДСТАВЛЕНИЯ ГБ-ФУНКЦИИ

Доказательство теоремы 4. а) Функция $F(x)$ является ГБ-функцией тогда и только тогда, когда для любого $\sigma \in \mathbf{Z}^*_{q^n-1}$ функция $F(x^\sigma)$ есть бент-функция. Поэтому для доказательства утверждения (а) достаточно показать, что если условие (1.16) не выполнено, то для некоторого $\sigma \in \mathbf{Z}^*_{q^n-1}$ функция $F(x^\sigma)$ не является бент-функцией. Для этого, согласно теореме 2, достаточно доказать, что редуцированный многочлен $\Phi_\sigma(x)$, представляющий многочлен $F(x^\sigma)$ равенством

$$F(x^\sigma) = \mathrm{tr}_P^Q(\Phi_\sigma(x)), \tag{3.1}$$

удовлетворяет условию

$$\mathrm{ind}_2\, \Phi_\sigma(x) > \lambda l. \tag{3.2}$$

Опишем вид функции $\Phi_\sigma(x)$. Нетрудно видеть, что для чисел $j, k \in M$ из условия $\rho(j\sigma) \equiv \rho(k\sigma)q^s \pmod{q^n-1}$ вытекает, что $j\sigma \equiv k\sigma q^s \pmod{q^n-1}$, $j \equiv kq^s \pmod{q^n-1}$ и, следовательно, $j = k$.

С учетом введенных обозначений это свойство означает, что числа $\rho(j\sigma), \rho(k\sigma)$ принадлежат различным циклотомическим классам, т. е. $\mu(\rho(j\sigma)) \neq \mu(\rho(t\sigma))$. Другими словами, функция $\mu(\rho(y\sigma))$ задает подстановку на M.

Теперь редуцированный многочлен $\Phi_\sigma(x)$ можно представить в виде

$$\Phi_\sigma(x) = \sum_{t \in M} c'_t \xi_t x^t, \tag{3.3}$$

где $c'_t = c_k^{q^{l_k}}$, а числа $k \in M$, $l_k \in \{0, \ldots, n-1\}$ — решения y и z уравнений соответственно:

$$t = \mu(\rho(y\sigma)), \quad t \equiv q^z \rho(k\sigma) \pmod{q^n-1}. \tag{3.4}$$

При этом в силу сделанных выше замечаний число ненулевых слагаемых в многочлене $\Phi_\sigma(x)$ будет таким же, как и в многочлене $\Phi(x)$, а набор весов $\{\|t\|_2 \colon t \in M, c'_t \neq 0\}$ совпадает с набором весов $\{\|\rho(k\sigma)\|_2 \colon k \in M, c_k \neq 0\}$. Таким образом,

$$S(\Phi_\sigma) = \{\mu(\rho(k\sigma)) \colon k \in S(\Phi)\}, \quad \operatorname{ind}_2 \Phi_\sigma(x) = \max\{\|\rho(k\sigma)\|_2 \colon k \in S(\Phi)\}. \tag{3.5}$$

Если включение (1.16) не выполняется, то возможна одна из двух ситуаций.

i) Для некоторых $k \in S(\Phi)$, $\sigma \in \mathbf{Z}^*_{q^n-1}$ выполняется неравенство $\|\rho(k\sigma)\|_2 > l\lambda$. В таком случае из (3.5) следует (3.2).

ii) Для некоторых $k \in S(\Phi)$, $\tau \in \mathbf{Z}^*_{q^n-1}$ выполняются условия $\mu(\rho(k\tau)) = s$, $\|s\|_2 < l\lambda$. Положим $\sigma = \rho(\tau(q^n - 2))$. Тогда $\sigma \in \mathbf{Z}^*_{q^n-1}$,

$$\rho(k\sigma) \equiv k\tau(q^n - 2) \equiv s(q^n - 2) \equiv (q^n - 1)s - s \equiv (q^n - 1) - s \pmod{q^n - 1},$$

и ввиду условия $1 \leqslant (q^n - 1) - s \leqslant q^n - 2$ получаем: $\rho(k\sigma) = (q^n - 1) - s$,

$$\|\rho(k\sigma)\|_2 = \|q^n - 1 - s\|_2 = nl - \|s\|_2 > l\lambda.$$

Опять приходим к (3.2).

б) Равенства (1.18), (1.20) следуют из теоремы 2 и утверждения (а), если заметить, что все числа из $M_q^{q^n}(l\lambda)$ имеют двоичную норму $l\lambda$.

Доказательство теоремы 5. Следует отметить, что эта теорема и ее доказательство во многом повторяют результаты работы [7] о свойствах множества $M_2^{2^n}(\lambda)$.

Нам понадобится следующая лемма, доказательство которой изложено в [7].

Лемма 3.1 [7]. *Пусть* $a \in \{1, \ldots, 2^s\}$. *Тогда* $\|a(2^s - 1)\|_2 = s$.

а) Пусть $\lambda = st$. Тогда $q^n - 1 = (q^{2s} - 1)(1 + q^{2s} + \ldots + q^{2s(t-1)})$ и $k = \dfrac{q^n - 1}{q^s + 1}$ имеет вид

$$k = (q^s - 1) + q^{2s}(q^s - 1) + \ldots + q^{2s(t-1)}(q^s - 1).$$

Следовательно, $\|k\|_2 = t\|q^s - 1\|_2 = tls = l\lambda$. Пусть $\sigma \in \mathbf{Z}^*_{q^n-1}$. Если $\sigma = d(q^s + 1) + a$ — деление с остатком числа σ на $q^s + 1$, то $k\sigma = d(q^n - 1) + ka$ — деление с остатком числа $k\sigma$ на $q^n - 1$. Следовательно, $\rho(k\sigma) = ka$. Так как

$$ka = (q^s - 1)a + q^{2s}(q^s - 1)a + \ldots + q^{2s(t-1)(q^s-1)}a$$

и $1 \leqslant (q^s - 1)a \leqslant q^{2s} - 2$, то, используя лемму 3.1, получаем: $\|\rho(k\sigma)\|_2 = \|ka\|_2 = tls = l\lambda$.

б) С учетом леммы 3.1 достаточно показать, что для любого $\sigma \in \mathbf{Z}^*_{q^n-1}$ выполняется равенство

$$\|\rho((q^\lambda - 1)a\sigma)\|_2 = \lambda l.$$

Пусть $a\sigma = d(q^\lambda + 1) + b$ — деление с остатком числа $a\sigma$ на $q^\lambda + 1$. Тогда $(q^\lambda - 1)a\sigma = d(q^n - 1) + (q^\lambda - 1)b$ — деление с остатком числа $(q^\lambda - 1)a\sigma$ на $q^n - 1$. Следовательно, $\rho((q^\lambda - 1)a\sigma) = (q^\lambda - 1)b$ и $\|\rho((q^\lambda - 1)a\sigma)\|_2 = l\lambda$ по лемме 3.1.

в) Покажем сначала, что

$$\forall \tau \in \mathbf{Z}^*_{q^{tn}-1}\colon \|\rho_{q^{tn}-1}(mk\tau)\|_2 = tl\lambda. \tag{3.6}$$

Так как $q^{tn} - 1 = m(q^n - 1)$, то

$$\rho_{q^{tn}-1}(mk\tau) = m\rho_{q^n-1}(k\tau) = m\rho_{q^n-1}(k\rho_{q^n-1}(\tau)).$$

Так как $\rho_{q^n-1}(\tau) \in \mathbf{Z}^*_{q^n-1}$, то по определению множества $M(\lambda)$ выполняется равенство $\|\rho_{q^n-1}(k\rho_{q^n-1}(\tau))\|_2 = l\lambda$. Так как при этом $\rho_{q^n-1}(k\rho_{q^n-1}(\tau)) < q^n$, то $\|\rho_{q^{tn}-1}(mk\tau)\|_2 = \|m\rho_{q^n-1}(k\rho_{q^n-1}(\tau))\|_2 = tl\lambda$, т. е. верно (3.6).

Теперь остается доказать, что mk — наименьшее число в циклотомическом классе $\{mk, \rho_{q^{tn}-1}(mkq), \ldots, \rho_{q^{tn}-1}(mkq^{tn-1})\}$. Пусть $K = \rho_{q^{tn}-1}(mkq^s)$ — представитель этого циклотомического класса. Заметим, что K имеет вид $K = m\rho_{q^n-1}(kq^r)$, где r — остаток от деления числа s на n. Так как по определению множества M справедливо неравенство $k \leqslant \rho_{q^n-1}(kq^r)$, то $mk \leqslant K$.

Доказательство теоремы 6. Рассмотрим кольцо $R = \mathbf{Z}_{q^n-1}$. По условию имеет место равенство идеалов: $Rk = Rd$. По теореме Басса [2] существует такой обратимый элемент $\sigma \in R^*$, что $d = k\sigma$. Так как $d \neq 0$, то последнее равенство дает: $d = \rho(k\sigma)$. Следовательно $d \in [k]$. Если $d' \in [k]$ и d' делит $q^n - 1$, то $Rk = Rd'$ и $d = d'$, так как идеал Rk содержит единственный образующий, делящий $q^n - 1$, а именно наименьший ненулевой элемент из Rk.

СПИСОК ЛИТЕРАТУРЫ

1. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями. — Дискрет. матем., 1994, т. 6, в. 3, с. 216–226.

2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

3. *Солодовников В. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу. — Дискрет. матем., 2002, т. 14, в. 1, с. 99–113.

4. *Dilon J. F.* A survey of bent functions. — The NSA Technical Journal, 1972, p. 191–215.

5. *Rothaus O.S.* On «bent» functions. — J. Comb. Theory. Ser. A, 1976, v. 20, № 3, p. 300–305.

6. *Youssef A.M., Gong G.* Hyper-bent functions. — Lect. Notes. Comp. Sci., 2001, v. 2045, p. 406–419.

7. *Кузьмин А.С., Марков В.Т., Нечаев А.А., Шишков А.Б.* Приближение булевых функций мономиальными. — Дискрет. матем., 2006, т. 18, в. 1, с. 9–29.

8. *Кузьмин А.С., Нечаев А.А., Шишкин В.А.* Бент- и гипербент-функции над полем из 2^l элементов. — В сб.: Труды по дискретной математике. Т. 9. — М.: Гелиос АРВ, 2006, с. 86–111.

9. *Kuzmin A.S., Markov V.T., Nechaev A.A., Shishkin V.A., Shishkov A.B.* Bent- and hyperbent-functions over a field of 2^l elements. — Proc. X Int. Workshop ACCT-X, 2007.