

В. А. Ш и ш к и н (Москва, ТВП). **Приближение 2^l -значных функций некоторыми системами статистических аналогов индекса нелинейности 2.**

Пусть $P = \mathbf{F}_q$, $Q = \mathbf{F}_{q^n}$ — расширение поля P , $q = 2^l$. Рассматривается задача приближения произвольной функции $F: Q \rightarrow P$ функцией из некоторого ограниченного класса $\mathcal{A}$ функций того же вида.

Пусть $N_a(F) = |\{x \in Q: F(x) = a \in P\}|$. Для оценки эффективности замены функции F некоторым ее аналогом $A: Q \rightarrow P$ используется функция *согласия*:

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

Возможности аппроксимации функции $F: Q \rightarrow P$ функциями из некоторого класса $\mathcal{A}$ и возможности класса $\mathcal{A}$ приближать произвольную функцию из P^Q характеризуются, соответственно, следующими параметрами:

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

В качестве класса $\mathcal{A}$ аппроксимирующих функций рассматривается один из следующих.

1. Класс $\mathcal{H} = \text{Hom}_{\mathbf{Z}}(Q, P)$ всех гомоморфизмов $h: (Q, +) \rightarrow (P, +)$.
2. Класс $\mathcal{QH} = \mathcal{QH}(Q, P)$ функций вида $g(x) = h_{\mathbf{a}_1}(x)h_{\mathbf{a}_2}(x) + h_{\mathbf{b}}(x)$, $h_{\mathbf{a}_1}, h_{\mathbf{a}_2}, h_{\mathbf{b}} \in \mathcal{H}$.
3. Класс $\mathcal{MH}_k = \mathcal{MH}_k(Q, P)$, где $k \in \mathbf{Z}_{q^n-1}$, функций вида $g(x) = h_{\mathbf{a}}(x) + h_{\mathbf{b}}(x^k)$, $h_{\mathbf{a}}, h_{\mathbf{b}} \in \mathcal{H}$.

Теорема 1. Пусть $n > 2$. Тогда для системы статистических аналогов $\mathcal{QH}$ справедлив следующий результат: $\nabla^2 \mathcal{QH} \geq q^{-n} + 2/q^{2n}$, в частности, $\nabla \mathcal{QH} > q^{-n/2}$.

Теорема 2. Если $\text{НОД}(n, s) = 1$, то $\nabla \mathcal{MH}_{1+q^s} > q^{-n/2}$.

Пусть $H_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}}(x) = h_{\mathbf{a}_1}(x)h_{\mathbf{a}_2}(x) + h_{\mathbf{b}}(x) \in \mathcal{QH}$, $h_{\mathbf{a}_1}, h_{\mathbf{a}_2}, h_{\mathbf{b}} \in \mathcal{H}$, тогда для величины $N_a(F + H_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}})$ имеет место следующее соотношение.

Теорема 3. Пусть $F \in P^Q$, $H_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}}(x) = h_{\mathbf{a}_1}(x)h_{\mathbf{a}_2}(x) + h_{\mathbf{b}}(x) \in \mathcal{QH}$, $h_{\mathbf{a}_1}, h_{\mathbf{a}_2}, h_{\mathbf{b}} \in \mathcal{H}$. Тогда для любых $a \in P$ и $\xi \in P \setminus \{0\}$ выполняется следующее соотношение:

$$N_a(F + H_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}}) = \frac{1}{q} \sum_{s_1, s_2 \in P} N_a(F + H_{s_1 s_2}) + q^{n-1} - q^n,$$

где $H_{s_1 s_2}(x) = s_1 h_{\mathbf{a}_1}(x) + s_2 h_{\mathbf{a}_2}(x) + h_{\mathbf{b}}(x) + s_1 s_2$.

Так как $H_{s_1, s_2} \in \mathcal{H}$, то теорема 3 позволяет вычислять значения величин $N_a(F + H_{\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}})$ через значения соответствующих величин для приближения функции F некоторыми гомоморфизмами из $\mathcal{H}$. Кроме этого, из теоремы 3 вытекает важное следствие.

Следствие 1. Пусть $F \in P^Q$ — бент-функция (см. [1], [2]) и $n > 2$. Тогда выполняется неравенство $\nabla^2(F, \mathcal{QH}) \geq q^{-n} + 2(q^{n+2}(q-1))^{-1}$.

Для функции $F \in P^Q$ обозначим $F|_R$ ограничение функции F на множество $R \subseteq Q$. Обозначим $\Delta_d F$ функцию из P^Q , действующую на элементах Q следующим образом: $\Delta_d F(x) = F(x) + F(x+d)$.

Предложение 1. Пусть $F \in P^Q$, тогда для всех $d \in Q \setminus \{0\}$ выполняется:

$$\nabla^2(F, \mathcal{MH}_{1+q^s}) \geq q^{-n} + \frac{1}{q^{2n-1}(q-1)} \left(N_0(\Delta_d F|_R) - q^{\text{НОД}(n, s)-1} \right),$$

где

$$R = \begin{cases} dK, & \text{если } \text{НОД}(n, 2s) = \text{НОД}(n, s), \\ d(z+K), & \text{если } \text{НОД}(n, 2s) = 2\text{НОД}(n, s), \end{cases}$$

$K = \mathbf{F}_{q^{\text{НОД}(n,s)}}$, $z \in K' = \mathbf{F}_{q^{2\text{НОД}(n,s)}}$ такое, что $\text{tr}_K^{K'}(z) = 1$.

Предложение 2. Пусть $F \in P^Q$ и $\text{НОД}(n, 2s) = \text{НОД}(n, s)$, тогда

$$\nabla^2(F, \mathcal{MH}_{1+q^s}) \geq q^{-n} + \frac{q^{\text{НОД}(n,s)}}{q^{2n}(q^{\text{НОД}(n,s)} - 1)} \left(q^{\text{НОД}(n,s)} \nabla^2(F|_K, 0) - 1 \right),$$

более того,

$$\nabla^2(F, \mathcal{MH}_{1+q^s}) \geq q^{-n} + \frac{q^{\text{НОД}(n,s)}}{q^{2n}(q^{\text{НОД}(n,s)} - 1)} \left(q^{\text{НОД}(n,s)} \nabla^2(F|_K, \mathcal{H}|_K) - 1 \right),$$

где $K = \mathbf{F}_{q^{\text{НОД}(n,s)}}$, $\mathcal{H}|_K$ — множество всех гомоморфизмов групп $h : (K, +) \rightarrow (P, +)$.

Из предложения 2 вытекают следующие следствия.

Следствие 2. Пусть $F \in P^Q$, $\text{НОД}(n, 2s) = \text{НОД}(n, s)$ и функция F линейна на подполе $K = \mathbf{F}_{q^{\text{НОД}(n,s)}}$ поля Q . Тогда $\nabla^2(F, \mathcal{MH}_{1+q^s}) \geq q^{-n} + q^{\text{НОД}(n,s)-2n}$.

Следствие 3. Если $\text{НОД}(n, 2s) = \text{НОД}(n, s)$ и $F|_K \in P^K$ не является бент-функцией, то $\nabla(F, \mathcal{MH}_{1+q^s}) > q^{-n/2}$.

Работа поддержана грантом Президента РФ № НШ-8564.2006.10.

СПИСОК ЛИТЕРАТУРЫ

1. 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. — In: Proceedings of the X-th Int. Worksh. on Algebr. and Combin. Coding Theory. Zvenigorod, 2006, p. 178–181.
2. Solodovnikov V. I. Bent-functions over a finite Abelian group. — Дискретн. матем., 2002, v. 14, № 1, p. 99–113.