М. М. Глухов, П. Н. Закревский (Москва, ТВП)**. О коэффициентах аддитивности и аффинности дискретных функций.**

Введем обозначения: $(H,+),(G,+)$ — конечные группы; H^G — множество всех отображений G в H; $\|f\|$ — вес функции F; $N_b^f = |\{a \in G\colon\ f(a) = b\}|$ — число векторов из G, на которых функция f принимает значение, равное b; V_n — пространство строк длины n над полем $\mathbf{P} = \mathrm{GF}(2)$, $V_n^0 = V_n \setminus \{0\}$; F_n — множество всех булевых функций от n переменных; L_n — множество всех линейных булевых функций от n переменных; A_n — множество всех аффинных булевых функций от n переменных; $V_n^{(i)}(f,g)$ — множество векторов из V_n, на котором значения функций f и g совпадают ($i=0$) или не совпадают ($i=1$).

О п р е д е л е н и е 1. *Коэффициентом аддитивности функции* $f \in H^G$ назовем число

$$\mathrm{Add}\,(f) = \frac{|\{(x,y) \in G^2\colon\ f(x+y) = f(x)+f(y)\}|}{|G|^2}.$$

О п р е д е л е н и е 2. *Коэффициентом аффинности функции* $f \in H^G$ назовем число

$$\mathrm{Aff}\,(f) = \max_{a \in H} \frac{|\{(x,y) \in G^2\colon\ f(x+y) = f(x)+f(y)+a\}|}{|G|^2}.$$

Укажем простейшие свойства коэффициента аффинности: 1) $1/\|H\| \leqslant \mathrm{Aff}\,(F) \leqslant 1$; 2) $\mathrm{Aff}\,(f) = 1 \iff f$ — аффинная функция; 3) $\forall c \in H$: $\mathrm{Aff}\,(f) = \mathrm{Aff}\,(f+c)$; 4) $\forall g(x) \in \mathrm{Hom}\,(G,H)$: $\mathrm{Aff}\,(f) = \mathrm{Aff}\,(f+h)$; 5) $\forall \varphi \in \mathrm{Aut}\,(G)$: $\mathrm{Aff}\,(f) = \mathrm{Aff}\,(f \circ \varphi)$, где $\circ$ — знак композиции функций.

Заметим, что идея сравнения функций на группах с гомоморфизмами групп впервые на вероятностном языке была использована А. С. Амбросимовым в 1981 г. В частности, им для функций от n переменных над кольцами вычетов и конечными полями найдены вероятности аддитивности $\mathbf{P}\{f(\sum_{i=1}^l x_i) = \sum_{i=1}^l f(x_i)\}$ функции f в общем случае, а также в случаях, когда f является бент-функцией, при условии, что элементы x_i выбираются случайно независимо и равновероятно из области определения функции f. Отсюда для булевых бент-функций

$$\mathrm{Add}\,(f) = \begin{cases} \dfrac{1}{2} + \dfrac{1}{2^{n+1}}, & \text{если } f(0) = 0, \\ \dfrac{1}{2} - \dfrac{1}{2^{n+1}}, & \text{если } f(0) = 1. \end{cases}$$

В работах [1–4] для $f \in H^G$ при любых группах H, G свойство $f(a+b) = f(a)+f(b)$ положено в основу теста на близость функции f к гомоморфизмам групп. В них величина $\mathrm{Err}\,(f) = \mathbf{P}\{f(u+v) \neq f(u)+f(v)\}$ сравнивалась с расстоянием функции f до класса гомоморфизмов. Имеются оценки разности сравниваемых величин.

Ниже приводятся результаты авторов данного доклада.

Пусть $f \in H^G$, $f_a(x) = \chi_a(f(x))$, где χ_a — комплексный характер группы H, соответствующий элементу a. Обозначим η_b^G характер группы G, соответствующий b, и разложим функцию f_a в ряд Фурье по характерам группы G: $f_a(x) = \sum_{b \in G} C_b^{f_a} \eta_b^G(x)$.

Систему комплексных чисел $C_b^{f_a}$, где $a \in H$, $b \in G$, называют *спектром функции* f_a. Из ортогональности характеров следует, что $C_b^{f_a} = |G|^{-1} \sum_{x \in G} f_a(x) \overline{\eta}_b^G(x)$, где $\overline{\eta}_b^G$ — характер, сопряженный с η_b^G.

Теорема 1. *Пусть* $f\colon\ G \to H$, *где* $G = (Z/q)^n$, $H = (Z/q)^l$ — *прямые суммы аддитивной группы* Z/q. *Тогда имеет место равенство*

$$\mathrm{Add}\,(f) = \frac{1}{|H|} \sum_{a \in H} \sum_{b \in G} C_b^{f_a} |C_b^{f_a}|^2.$$

Следствие 1. *Если f из теоремы* 1 *является бент-функцией, то*

$$\mathrm{Add}\,(f)=\begin{cases}\dfrac{1}{|H|}+\dfrac{|H|-1}{|G|\,|H|}, & \text{если } f(0)=0,\\ \dfrac{1}{|H|}-\dfrac{1}{|G|\,|H|}, & \text{если } f(0)\neq 0.\end{cases}$$

З а м е ч а н и е. Частными случаями теоремы 1 и ее следствия 1 являются результаты А. С. Амбросимова при $l=2$.

Всюду далее речь будет идти о булевых функциях из F_n.

Следствие 2. *Для булевой функции $f\in F_n$:*

$$\mathrm{Add}\,(f)=\frac{1}{2}+\frac{1}{2}\sum_{a\in V_n}(W_a^f)^3,$$

где $W_a^f=2^{-n}\sum_{x\in V_n}(-1)^{f(x)+(a,x)}$ есть коэффициент Уолша–Адамара функции f.

Теорема 2. *Пусть $f\in F_n$, $\|f\|=k$, $N_1^f=\{c_1,c_2,\dots,c_k\}$, M — множество из m-неупорядоченных троек $\{a,b,c\}$ с элементами $a,b,c\in N_1^f\setminus\{0\}$, удовлетворяющими условию $a+b+c=0$. Тогда* $\mathrm{Aff}\,(f)=\max\{\mathrm{Add}\,(f),1-\mathrm{Add}\,(f)\}$ *и*

$$\mathrm{Add}\,(f)=1-\frac{6}{2^{2n}}\left(2^{n-1}k-(k-i)^2+4m-\frac{i}{3}\right),\quad \text{где}\ \ i=f(0).$$

Следствие 3. *Для любой функции $f\in F_n$ веса k имеют место неравенства*

$$\mathrm{Aff}\,(f)=\begin{cases}\dfrac{1}{2}+\dfrac{1}{2^{n-3}}, & \text{если } f(0)=0,\ k=0\,(\mathrm{mod}\,2),\\ \dfrac{1}{2}+\dfrac{1}{2^{n-3}}-\dfrac{3}{2^{2n-1}}, & \text{если } f(0)=0,\ k=1\,(\mathrm{mod}\,2),\\ \dfrac{1}{2}+\dfrac{1}{2^{n-3}}, & \text{если } f(0)=1,\ k=0\,(\mathrm{mod}\,2),\\ \dfrac{1}{2}+\dfrac{1}{2^{n-3}}+\dfrac{1}{2^{2n-1}}, & \text{если } f(0)=1,\ k=1\,(\mathrm{mod}\,2),\end{cases}$$

причем достигаться указанные оценки могут лишь при $m=m_0+\Delta$, где

$$m_0=\frac{2^{2n-4}}{3}-\frac{(2^{n-1}-k)k}{4},\quad \Delta\in\left\{-\frac{1}{3},\frac{7}{12},-\frac{2k-1}{4}+\frac{5}{12},-\frac{2k-1}{4}+\frac{2}{3}\right\}.$$

Вопрос о достижимости оценок в общем виде остается открытым.

Теорема 3. *Пусть $f(x)=\prod_{l=1}^{k}(a_l,x)$ $(1\leqslant k\leqslant 2^n)$ — мультилинейная функция из F_n, $(a_1,a_2,\dots,a_r)$ $(1\leqslant r\leqslant k)$—- максимальная линейно независимая подсистема системы векторов $(a_1,a_2,\dots,a_k)$ и $a_j=\sum_{i=1}^{r}c_i^j a_i$ при $j\in\{r+1,\dots,k\}$ и $c_j=(c_1^j,c_2^j,\dots,c_r^j)$. Тогда*

$$\mathrm{Aff}\,(f)=\begin{cases}\max\left\{\dfrac{1}{2}\pm\dfrac{2^{2r-2}-3(2^{r-1}-1)}{2^{2r-1}}\right\}, & \text{если } \forall j\in\{r+1,\dots,k\}\colon\ \|c_j\|=1\,(\mathrm{mod}\,2),\\ 1, & \text{если } \exists j\in\{r+1,\dots,k\}\colon\ \|c_j\|=0\,(\mathrm{mod}\,2).\end{cases}$$

Теорема 4. *Для любых различных функций $f,g\in F_n$ (обозначив $\mathbf{V}=V_n^{(1)}(f,g)$) имеем*

$$\mathrm{Add}\,(f)-\mathrm{Add}\,(g)=\frac{3}{2^{2n}}\sum_{z\in\mathbf{V}}(-1)^{f(z)}\Delta_f(z)-\frac{3}{2^{2n-1}}\sum_{z\in\mathbf{V}}\sum_{y\in\mathbf{V}}(-1)^{f(z)+f(y)+f(z+y)}$$
$$+\frac{1}{2^{3n-2}}\sum_{x\in\mathbf{V}}\sum_{y\in\mathbf{V}}\sum_{z\in\mathbf{V}}(-1)^{f(z)+f(y)+f(x)}\sum_{\alpha\in V_n}(-1)^{(\alpha,x+y+z)}.$$

Здесь $\Delta_f(u) = \sum_{x \in V_n} (-1)^{f(x+u)+f(x)}$ *есть автокорреляционная функция для* $f \in F_n$.

Следствие 4. *Если* $f, f_i \in F_n$, f *— бент-функция и* $|N_1^{f_i} - N_1^f| \equiv i$, *то, обозначив* $\mathbf{A} \equiv \mathrm{Add}\,(f) - \mathrm{Add}\,(f_i)$ *и* $\mathbf{V} \equiv V_n^{(1)}(f, f_1)$, *имеем*:
при $i = 1$

$$\mathbf{A} = \begin{cases} \dfrac{3 \cdot 2^{n-1} - 1}{2^{2n-1}}(-1)^{f(0)}, & \text{если } \mathbf{V} = \{0\}, \\ \dfrac{3 \cdot 2^{n-1}}{2^{2n-1}}(-1)^{f(0)+1}, & \text{если } \mathbf{V} = \{\gamma\}; \end{cases}$$

при $i = 2$

$$\mathbf{A} = \begin{cases} \dfrac{3 \cdot 2^{n-1} - 4}{2^{2n-1}}(-1)^{f(0)}, & \text{если } \mathbf{V} = \{0, \gamma\}, \\ -\dfrac{6}{2^{2n-1}}\left((-1)^{f(0)} + (-1)^{f(\gamma_1)+f(\gamma_2)+f(\gamma_1+\gamma_2)}\right), & \text{если } \mathbf{V} = \{\gamma_1, \gamma_2\}; \end{cases}$$

при $i = 3$ *и дополнительном обозначении* $\mathbf{f} \equiv f(\gamma_1) + f(\gamma_2)f(\gamma_1 + \gamma_2)$

$$\mathbf{A} = \begin{cases} \dfrac{3 \cdot 2^{n-1} - 7}{2^{2n-1}}(-1)^{f(0)} - \dfrac{6}{2^{2n-1}}(-1)^{\mathbf{f}}, & \text{если } \mathbf{V} = \{0, \gamma_1, \gamma_2\}, \\ \dfrac{3}{2^{2n-1}}\left((-1)^{f(0)} + 2(-1)^{\mathbf{f}}\right), & \text{если } \mathbf{V} = \{\gamma_1, \gamma_2, \gamma_3 | \gamma_1 + \gamma_2 = \gamma_3\}, \\ -\dfrac{3}{2^{2n-1}}\left(3(-1)^{f(0)} + 2\sum\limits_{1 \leqslant i < j \leqslant 3}(-1)^{\mathbf{f}}\right), & \text{если } \mathbf{V} = \{\gamma_1, \gamma_2, \gamma_3 | \gamma_1 + \gamma_2 \neq \gamma_3\}. \end{cases}$$

СПИСОК ЛИТЕРАТУРЫ

1. *Bellare M.*, *Goldwasser S.*, *Lund C.*, *Russell A.* Efficient probabilistically checkable proofs and applications to approximation. — In: Proceedings of the 25th Annual Symp. on Theory of Computing, ACM, 1993.
2. *Bellare M.*, *Coppersmith D.*, *Hastad J.*, *Kiwi M.*, *Sudan M.* Linearity Testing in Characteristic Two. — IEEE Trans. on Information Theory, 1996, v. 42, № 6, p. 1781–1795.
3. *Blum M.*, *Luby M.*, *Rubinfeld R.* Self-Testings/Correcting with Applications to Numerical Problems. — J. of Computer and System Sciences, 1993, v. 47, p. 549–595.
4. *Kaufman T.*, *Litsyn S.*, *Xie N.* Breaking the ε-Soundness Bound of the Linearity Test over GF(2). — SIAM Journal on Computing, 2010, v. 39, № 5, p. 1988–2003.