**А. М. З у б к о в**, **А. А. С е р о в** (Москва, МИАН, ЗТ). **Среднее число подфункций случайной булевой функции, близких к множеству аффинных функций.**

Пусть $\mathbf{F}_2^n$ и $A_n$ — множества всех булевых и всех аффинных функций от $n$ булевых переменных соответственно, и $\mathbf{F}_2^n(r)$ ($\mathbf{F}_2^n(r) \subseteq \mathbf{F}_2^n$) — множество булевых функций, расстояние Хэмминга от которых до множества $A_n$ не превосходит $r$ (см. [1]).

Пусть $f(x_1, x_2, \ldots, x_n) \in \mathbf{F}_2^n$. Множеству $I_n^s = \{i_1 < i_2 < \cdots < i_s\} \subset \{1, 2, \ldots, n\}$ и набору констант $C_n(I_n^s) = \{c_j \in \mathbf{F}_2,\ j \in \{1, 2, \ldots, n\} \backslash I_n^s\}$ соответствуют вектор $(z_1, z_2, \ldots, z_n)$, в котором

$$z_j = \begin{cases} c_j & \text{при } j \in \{1, 2, \ldots, n\} \backslash I_n^s, \\ y_k & \text{при } j = i_k \in I_n^s, \end{cases}$$

и *подфункция* $g(I_n^s, C_n(I_n^s); y_1, y_2, \ldots, y_s) = f(z_1, z_2, \ldots, z_n)$ булевой функции $f(x_1, x_2, \ldots, x_n)$.

Для функции $f \in \mathbf{F}_2^n$ обозначим $\nu(f, s, r)$ число ее подфункций от $s$ переменных, находящихся на расстоянии не больше $r$ от множества $A_s$, т. е число таких пар $(I_n^s, C_n(I_n^s))$, что $g(I_n^s, C_n(I_n^s)) \in \mathbf{F}_2^s(r)$.

**Утверждение.** *Если $\varphi$ — случайная булева функция, равновероятно распределенная на $\mathbf{F}_2^n$, то при $r < 2^{s-2}$*

$$\mathbf{E}\,\nu(\varphi, s, r) = C_n^s\, 2^{n-2^s+1} \sum_{j=0}^{r} C_{2^s}^j.$$

Из этого равенства следуют оценки

$$2^{n-2^s+1} C_n^s C_{2^s}^r \leqslant \mathbf{E}\,\nu(\varphi, s, r) \leqslant 2^{n+1}\, C_n^s \left(\frac{2}{3}\right)^{2^{s-2}},$$

в которых при $n \to \infty$ левая часть стремится к бесконечности, если $s \leqslant \log_2 n$, а правая часть стремится к 0, если $s \geqslant \log_2 n + 3$; таким образом, при $n \to \infty$ «пороговым» являются значение $s$, лежащее в интервале от $\log_2 n$ до $\log_2 n + 3$.

СПИСОК ЛИТЕРАТУРЫ

1. *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.