А. А. С е р о в (Москва, МИАН)**. Оценки числа булевых функций, имеющих квадратичные приближения заданной точности.**

Пусть $\mathbf{F}_2$ — поле из двух элементов, $V_n = \mathbf{F}_2^n$ есть пространство n-мерных векторов с компонентами из $\mathbf{F}_2$. В множестве $\mathbf{F}_2^{V_n}$ всех булевых функций от n булевых переменных рассмотрим класс квадратичных функций

$$\mathbf{Q}_n = \Big\{ f \in \mathbf{F}_2^{V_n} : f(x_1, x_2, \ldots, x_n) = \bigoplus_{1 \leqq i < j \leqq n} b_{ij} x_i x_j \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus a_0,\ b_{ij}, a_i \in \mathbf{F}_2 \Big\}$$

где $\oplus$ — сложение в $\mathbf{F}_2$.

Из результатов [1] следует, что если $\mathbf{F}_2(\mathbf{Q}_n, r) = \{ f \in \mathbf{F}_2^{V_n} : \rho(f, \mathbf{Q}_n) \leqq r \}$ есть множество булевых функций, расстояние Хэмминга от которых до класса $\mathbf{Q}_n$ не превосходит натурального $r \leqq 2^{n-1}$, то при $n \to \infty$

$$\sup_{0 \leqq r < 2^{n-1} - \sqrt{2^{n-2} \ln 2}} \Big| 2^{-2^n} |\mathbf{F}_2(\mathbf{Q}_n, r)| - \Big(1 - e^{-e^{-x(n,r)}} \Big) \Big| \to 0,$$

где $x(n, r)$ — решение некоторого уравнения, и для любого $\varepsilon > 0$

$$\lim_{n \to \infty} 2^{-2^n} \Big| \mathbf{F}_2 \Big(\mathbf{Q}_n, 2^{n-1} - (1 + \varepsilon) n \sqrt{2^{n-2} \ln 2} \Big) \Big| = 0,$$

$$\lim_{n \to \infty} 2^{-2^n} \Big| \mathbf{F}_2 \Big(\mathbf{Q}_n, 2^{n-1} - (1 - \varepsilon) n \sqrt{2^{n-2} \ln 2} \Big) \Big| = 1,$$

Следующая теорема дополняет результаты [1].

Теорема. *Если* $n \geqq 3$, *то*

$$\Big(1 - Q(n, r) \Big) 2^{C_n^2 + n + 1} \sum_{m=0}^{r} C_{2^n}^m \leqq |\, \mathbf{F}_2(\mathbf{Q}_n, r)| \leqq 2^{C_n^2 + n + 1} \sum_{m=0}^{r} C_{2^n}^m,$$

где $Q(n, r) = 0$ *при* $0 \leqq r < 2^{n-3}$,

$$Q(n, r) < \frac{2^{-n^2 (c_r^2 - 3)/6 + n + 1}}{n^2} \exp \left\{ \frac{(c_r n)^3}{7 \cdot 2^{n/2}} \right\}$$

при $n \geqq 15$ *и* $r = 2^{n-1} - c_r n \sqrt{2^{n-2} \ln 2} \geqq 0$, $c_r > 1$.

З а м е ч а н и е. Неравенства теоремы позволяют получать оценки для левого хвоста распределения расстояния от случайной булевой функции до множества квадратичных булевых функций.

Отношения верхних и нижних оценок в теореме стремятся к 1, если $n \to \infty$ и $r < 2^{n-1} - c\, n \sqrt{2^{n-2} \ln 2}$, $c > \sqrt{3} = 1,7321 \ldots$

Явные верхние и нижние оценки для сумм $\sum_{m=0}^{r} C_{2^n}^m$ при $r \leqq 2^{n-1}$ приведены в [2].

Следствие. *Если* $c > 1$ *и* $n, r \to \infty$ *так, что выполняется условие* $r < 2^{n-1} - c \sqrt{2^{n-2}(n^2 + n) \ln 2}$, *то при достаточно больших* n

$$\frac{|\mathbf{F}_2(\mathbf{Q}_n, r)|}{2^{2^n}\ (1 - e^{-e^{-x(n,r)}})} < \frac{1,5}{c}\,.$$

Работа поддержана РФФИ, проект № 11-01-00139.

СПИСОК ЛИТЕРАТУРЫ

1. *Рязанов Б. В., Чечёта С. И.* О приближении случайной булевой функции множеством квадратичных форм. — Дискретн. матем., 1995, т. 7, в. 3, с. 129–145.

2. *Зубков А. М., Серов А. А.* Оценки числа булевых функций, имеющих аффинные приближения заданной точности. — Дискретн. матем., 2010, т. 22, в. 4, с. 3–19.