А. М. З у б к о в, **А. А. С е р о в** (Москва, МИАН, ЗТ). **Оценки числа булевых функций, имеющих аффинные приближения заданной точности.**

Пусть $\mathbf{F}_2^n$ и A_n — множества всех булевых и всех аффинных функций от n булевых переменных соответственно, и $\mathbf{F}_2^n(r) \subseteq \mathbf{F}_2^n$ — множество булевых функций, расстояние Хэмминга от которых до множества A_n не превосходит r. Известно [1], что $\mathbf{F}_2^n(r) = \mathbf{F}_2^n$, если $r \geqslant 2^{n-1} - 2^{n/2-1}$. Из [2] следует, что если $\mathbf{F}_2^{n,0}(r)$ — множество всех булевых функций, расстояние Хемминга от которых до множества линейных функций (аффинных с нулевым свободным членом) не превосходит r, то при $n \to \infty$

$$2^{-2^n}|\mathbf{F}_2^{n,0}(r_n)| \to 1 - e^{-e^{-x}}, \quad x \in \mathbf{R},$$

если $r_n = 2^{n-1} - \sqrt{2^{n-1}(n\ln 2 - \ln(4\pi n \ln 2)/2 + x + o(1))}$, т. е. для основной массы булевых функций от n переменных расстояние до множества линейных функций близко к $2^{n-1} - \sqrt{n2^{n-1}\ln 2}$.

Здесь приводятся точные формулы и неравенства для $|\mathbf{F}_2^n(r)|$. Аналогичные результаты можно получить и для $|\mathbf{F}_2^{n,0}(r)|$.

Теорема. a) *Если* $0 < r < 2^{n-2}$, *то*

$$|\mathbf{F}_2^n(r)| = 2^{n+1}N_1(n,r), \quad \textit{где} \quad N_1(n,r) = \sum_{m=0}^{r} C_{2^n}^m.$$

b) *Если* $2^{n-2} \leqslant r < 2^{n-2} + 2^{n-4}$, *то*

$$|\mathbf{F}_2^n(r)| = 2^{n+1}N_1(n,r) - 4C_{2^n}^2 N_2(n,r) + 8C_{2^n}^3 N_3(n,r),$$

где

$$N_2(n,r) = \sum_{m_0=0}^{r-2^{n-2}} C_{2^{n-1}}^{m_0} \sum_{m_1=2^{n-1}-(r-m_0)}^{r-m_0} C_{2^{n-1}}^{m_1},$$

$$N_3(n,r) = \sum_{v=0}^{r-2^{n-2}} \sum_{u=2^{n-1}-r+2v}^{r} C_{2^{n-2}}^{v} C_{2^{n-2}}^{u-v} S(r-u, r+u-2v-2^{n-1}),$$

$$S(a,b) = \sum_{g+h\leqslant a,\, |g-h|\leqslant b} C_{2^{n-2}}^{g} C_{2^{n-2}}^{h}.$$

c) *Если* $r \geqslant 2^{n-2} + 2^{n-4}$, *то*

$$2^{n+1}N_1(n,r) - 4C_{2^n}^2 N_2(n,r) \leqslant |\mathbf{F}_2^n(r)| \leqslant 2^{n+1}N_1(n,r) - 4C_{2^n}^2 N_2(n,r) + 8C_{2^n}^3 N_3(n,r).$$

Для любого допустимого значения r вычисление $N_2(n,r)$ и $N_3(n,r)$ можно провести за $O(2^{2n})$ арифметических операций. Примеры, рассмотренные для случаев $n \leqslant 14$, показывают, что верхние и нижние оценки очень близки в широкой области значений r. Однако уже при умеренных n точные вычисления оказываются невозможными. Для $N_2(n,r)$ и $N_3(n,r)$ получены как приближенные (довольно громоздкие) формулы, так и оценки, например:

$$N_2(n,r) \leqslant C_{2^{n-1}}^{r-2^{n-2}} C_{2^{n-1}}^{2^{n-2}} \frac{1+q}{(1-q)^2}, \quad \text{где} \quad q = \frac{C_{2^{n-1}}^{r-2^{n-2}-1}}{C_{2^{n-1}}^{r-2^{n-2}}},$$

$$N_3(n,r) \leqslant 2^{2^n} \exp\left\{ -\frac{48r^2 - 9\,2^{n+2}r + 7\,2^{2n}}{2(2^n\,13/3 - 8r)} \right\}, \quad 2^{n-2} \leqslant r < 2^{n-2} + \frac{2^{n-2}}{3},$$

$$N_3(n,r) \leqslant 2^{2^n} \exp\left\{ -\frac{3(2^n-2r)^2}{2(2^n+2(2^n-2r))} \right\}, \quad 2^{n-2} + \frac{2^{n-2}}{3} \leqslant r \leqslant 2^{n-1}.$$

Из этих оценок следует, в частности, что

$$2^{-2^n} 8C_{2^n}^3 N_3\Big(n, 2^{n-1} - \sqrt{2^{n-1}(n + c\ln\ln n)\ln 2}\Big) < \frac{4}{3} 2^{-3c\ln\ln n}(1+\varepsilon_{n,c}),$$

$$2^{-2^n} 8C_{2^n}^3 N_3(n, 2^{n-1} - c\sqrt{2^{n-1} n \ln 2}) < \frac{4}{3} 2^{-3nc^2}(1+\delta_{n,c}),$$

где $\varepsilon_{n,c} = O\left(n^{3/2}/2^{n/2}\right)$ и $\delta_{n,c} = O\left(\sqrt{n}/2^{n/2}\right)$, $c > 0$, т. е. точность оценок из п. c) теоремы быстро возрастает с удалением r от $2^{n-1} - \sqrt{n2^{n-1}\ln 2}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
2. *Ryasanov B. V.* Probabilistic methods in the theory of approximation of discrete functions. — Probabilistic Methods in Discr. Math.: Proceedings of the Third International Petrozavodsk Conference. Moscow: TVP/VSP, 1993, p. 403–412.