А. А. С е р о в (Москва, МИАН)**. Оценки мощностей окрестностей двоичных дистанционно инвариантных кодов.**

Пусть $\mathcal{K}$ — двоичный дистанционно инвариантный код, т.е. такое подмножество пространства $\mathbf{F}_2^n$, что для любого $x \in \mathcal{K}$ совокупность расстояний Хемминга $\rho(x,y)$, $y \in \mathcal{K}\backslash\{x\}$, одинакова. Частными случаями дистанционно инвариантных кодов являются линейные коды и коды Рида–Маллера. Пусть $\mathbf{F}_2(\mathcal{K},r) = \{x \in \mathbf{F}_2^n\colon\ \rho(x,\mathcal{K}) \leqslant r\}$.

Представим, как в [1], окрестности кодовых слов в виде шаров целочисленного радиуса r. Если при $r=a$, $a \in \mathbf{N}_0$, шары не пересекаются, а при $r=a+1$ пересекаются, то a называется *радиусом сферической упаковки* кода. Минимальное значение b радиуса r, при котором $\mathbf{F}_2(\mathcal{K},b)=\mathbf{F}_2^n$, называется *радиусом покрытия* кода.

Нахождение значений $|\mathbf{F}_2(\mathcal{K},r)|$ представляет практический интерес, причем $|\mathbf{F}_2(\mathcal{K},r)| = 2^k\sum_{m=0}^{r} C_n^m$ при $r \leqslant a$ и $|\mathbf{F}_2(\mathcal{K},r)| = 2^n$ при $r \geqslant b$, а в случае $a<r<b$ соответствующие точные формулы весьма сложны.

Введем обозначения:

$$N_n^{(1)}(r) = \sum_{m=0}^{r} C_n^m, \quad N_n^{(2)}(m,r) = |\{x \in \mathbf{F}_2^n\colon\ \max\{\rho(0,x),\rho(c,x)\} \leqslant r, \rho(0,c)=m\}|.$$

Теорема. *Для любого двоичного дистанционно инвариантного кода $\mathcal{K}$ в $\mathbf{F}_2^n$ при $r \leqslant n$ справедливы оценки*

$$(1-q(n,r))|\mathcal{K}|\,N_n^{(1)}(r) \leqslant |\mathbf{F}_2(\mathcal{K},r)| \leqslant |\mathcal{K}|\,N_n^{(1)}(r),$$

где $q(n,r) = 2^{-1}\sum_{m=1}^{n}|W_m|N_n^{(2)}(m,r)/N_n^{(1)}(r)$ и $|W_m| = \{x \in \mathcal{K}\colon\ \rho(0,x)=m\}$, $m \in \{0,1,\dots,n\}$.

З а м е ч а н и е. Оценки теоремы аналогичны результатам [2].

Утверждение 1 см. [3]**.** *При $r \leqslant n/2$ справедливы оценки*

$$2^n\Phi\biggl(-\sqrt{nV\Bigl(1-\frac{2r}{n}\Bigr)}\biggr) \leqslant N_n^{(1)}(r) \leqslant 2^n\Phi\biggl(-\sqrt{nV\Bigl(1-\frac{2(r+1)}{n}\Bigr)}\biggr),$$

где $V(z) = (1-z)\ln(1-z)+(1+z)\ln(1+z)$.

Утверждение 2. *Если $0 \leqslant r \leqslant [n/2]$ и $0 \leqslant m \leqslant n$, то*

$$C_n^r(1+q) \leqslant N_n^{(1)}(r) \leqslant C_n^r\frac{1}{1-q}, \quad C_m^{[m/2]}N_{n-k}^{(1)}(r-[m/2]) \leqslant N_n^{(2)}(m,r),$$

где $q = r/(n-r+1)$.

Утверждение 3. *Если $0 \leqslant r \leqslant [n/2]$ и $0 \leqslant m \leqslant n$, то*

$$N_n^{(2)}(m,r) \leqslant \begin{cases} C_m^{m/2}C_{n-m}^{r-m/2}\dfrac{1+q_m}{(1-q_m)^2} & \text{при четном } m,\\ C_m^{[m/2]}C_{n-m}^{r-[m/2]}\dfrac{2}{(1-q_m)^2} & \text{при нечетном } m, \end{cases}$$

где $q_m = (r-[m/2])/(n-m+[m/2]-r+1) \leqslant q = r/(n-r+1)$.

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

СПИСОК ЛИТЕРАТУРЫ

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.
2. *Зубков А. М.*, *Серов А. А.* Оценки числа булевых функций, имеющих аффинные приближения заданной точности. — Дискретн. матем., 2010, т. 22, № 4, с. 3–19.
3. *Alfers D.*, *Dinges H.* A normal approximation for Beta and Gamma tail probabilities. — Z. Wahrscheinlichkeitstheorie verw. Gebiete, 1984, № 65, p. 399–420.