К. Н. П а н к о в (Москва, ТВП)**. Верхняя граница для числа платовидных двоичных отображений фиксированного порядка.**

Пусть $V_k = \{x_1, x_2, \ldots, x_k\}$ ($x_i \in \{0,1\}$) — множество двоичных векторов длины k. Множество всех отображений из V_n в V_m будем обозначать $B_{n,m}$. Можно рассматривать значение функции $f(\alpha) \in B_{n,m}$ как вектор $(f_1(\alpha), f_2(\alpha), \ldots, f_m(\alpha))$, компонентами которого являются значения ее координатных двоичных функций f_i, $i \in \{1,2,\ldots,m\} \equiv \mathbf{J}$ от n переменных.

Рассмотрим вектор $\overline{F} = \overline{F}(f,n,m,k) = (F_I^J,\ 0 \leqslant |I| \leqslant k,\ I \subset \{1,2,\ldots,n\} \equiv \mathbf{I},\ \varnothing \not\equiv J \subset \mathbf{J}$ размерности $L = L(n,m,k) = \sum_{s=1}^{m} \binom{m}{s} \sum_{i=0}^{k} \binom{n}{i}$, состоящий из первых спектральных коэффициентов Уолша $F_I^J = (1/2) \sum_{x \in V_n} (-1)^{(f^J)(x) \oplus x_{i_1} \oplus \cdots \oplus x_{i_{|I|}}}$ всех ненулевых линейных комбинация координатных функций функции f, где $J = \{j_1, j_2, \ldots, j_{|J|}\} \subset \mathbf{J}\}$, $I = \{i_1, i_2, \ldots, i_{|I|}\} \subset \mathbf{I}\}$, $f^J = f_{j_1} \oplus \cdots \oplus f_{j_{|J|}}$.

С помощью результатов [3] можно доказать следующее утверждение.

Утверждение. *Пусть $f = (f_1, f_2, \ldots, f_m) \in B_{n,m}$. Для любого непустого множества $J \subset \mathbf{J}$, для любого множества $I \subset \mathbf{I}$ выполняется*

$$\sum_{L \subset I,\ L \not\equiv I} (-1)^{|I \setminus L|+1} F_L^J \equiv F_I^J \ \left(\mathrm{mod}\ 2^{|I|}\right), \tag{1}$$

$$\sum_{\varnothing \neq S \subset J,\ L \subset I} (-1)^{|L|+|S|} F_L^S \equiv 0 \ \left(\mathrm{mod}\ 2^{|I|+|J|-1}\right). \tag{2}$$

Согласно [4], двоичная функция $f \in B_{n,1}$ называется *платовидной функцией порядка* $2r$, если квадрат каждого коэффициента Уолша равен по модулю либо $2^{2n-2r-2}$, либо 0.

Согласно [1], двоичное отображение из $B_{n,m}$ называется *платовидным*, если платовидны все ненулевые линейные комбинации его координатных функций.

Введем понятие *порядка* платовидного отображения, которым мы будем называть вектор $(r_J,\ \varnothing \neq J \subset \mathbf{J})$, составленный из порядков r_J ненулевых линейных комбинаций его координатных функций f^J, упорядоченный лексикографически по J. Множество платовидных отображений с таким порядком обозначим $\Pi\,(r_J,\ \varnothing \neq J \subset \mathbf{J})$.

Пусть далее функция f выбирается случайно и равновероятно из множества $B_{n,m}$. Тогда $\overline{F} = \overline{F}(f,n,m,k)$ является случайным вектором длины L.

Используя результаты работ [2], [3] и [5], можно найти распределение этого вектора. Отметим, что в формулировке основной теоремы [5] автором была допущена ошибка. Числитель дроби в формуле (1) должен выглядеть следующим образом:

$$\exp\left\{ -2^{2m-3} \sum_{\varnothing \neq J \subset \mathbf{J}} \sum_{I \subset \mathbf{I},\ |I| \leqslant k} \left(\sum_{K \subset I} (-1)^{|K|} 2^{|K|} z_K^J \right)^2 \right\} + O\left(n^{3k+3} 2^{-n/2+3m}\right).$$

Теорема 1. *Пусть $n \to \infty$, $k(n) = o\,(\sqrt{n})$, $m(n) = o\,(n)$. Тогда равномерно относительно векторов $\overline{a}$ длины $L(n,m,k)$, координаты которых удовлетворяют отношениям* (1), (2), *справедливо представление*

$$\mathbf{P}\,\{\overline{F} = \overline{a}\} = \left[\exp\left\{ -2^{-n+1} \sum_{\varnothing \neq J \subset \mathbf{J}} \sum_{I \subset \mathbf{I},\ |I| \leqslant k} (a_I^J)^2 \right\} + O\left(n^{3k+3} 2^{-n/2+3m}\right) \right]$$
$$\times \left[\exp\left\{ \left(\frac{n-k}{2} \binom{n}{k} (2^m - 1) - L(n,m,k)(m - \log_2 \sqrt{2\pi}) \right) \ln 2 \right\} \right]^{-1}.$$

Эта теорема обобщает для векторов растущей размерности результаты работы [6] и используется при доказательстве верхней границы для числа платовидных двоичных отображений фиксированного порядка.

Теорема 2. *Пусть при* $n \to \infty$ *выполняется* $k(n) = o(\sqrt{n})$, $m(n) = o(n)$. *Тогда при всех достаточно больших* n, *любом* $\varepsilon > 0$ *и произвольном наборе таких неотрицательных чисел* r_J, $\varnothing \neq J \subset \mathbf{J}$, *меньших* $n/2$, *что* $n/2 - r_J = o(\ln n)$

$$\log_2(|\Pi(r_J,\, \varnothing \neq J \subset \mathbf{J}|) < m2^n - \frac{n-k}{2}\binom{n}{k}(2^m - 1)$$
$$+ L\left(m + \log_2 \frac{3}{\sqrt{2\pi}}\right) - \frac{n}{2} + 3m + (3k + 3 + \varepsilon)\log_2 n.$$

СПИСОК ЛИТЕРАТУРЫ

1. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. New York: Cambridge University Press, 2010, 780 с.
2. *Canfield E. R.*, *Gao Z.*, *Greenhill C.*, *McKay B. D.*, *Robinson R. W.* Asymptotic enumeration of correlation-immune boolean functions. — Cryptography and Communications, 2010, v. 2, № 1, p. 111—126.
3. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции. — Дискретн. матем., 2000, т. 12, в. 1, с. 82–95.
4. *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004, 472 с.
5. *Панков К. Н.* Асимптотическая формула для числа корреляционно-иммунных порядка k и (n, m, k)-устойчивых функций. — Обозрение прикл. и промышл. матем., 2005, т. 12, в. 2, с. 461–462.
6. *Рязанов Б. В.* О распределении спектральной сложности булевых функций. — Дискретн. матем., 1994, т. 6, в. 2, с. 111–129.