ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 4
2012

А. М. Зубков, В. И. Куглов (Москва, МИ РАН)**. О весах двоичных векторов в случайных линейных подпространствах.**

Пусть $B_N = \mathrm{GF}(2)^N$ — двоичное N-мерное линейное пространство. *Весом* $w(X)$ двоичного вектора $X = (x_1, x_2, \ldots, x_N) \in B_N$ будем называть количество ненулевых координат в векторе X. Разобьем пространство B_N на множества векторов одинакового веса s, $0 \leqslant s \leqslant N$: $B_N^s = \{X \in B_N \,|\, w(X) = s\}$, $B_N = \bigsqcup_{s=0}^N B_N^s$. Обозначим $B_N^{\leqslant s} = \{X \in B_N \,|\, w(X) \leqslant s\}$ множество векторов веса, не превосходящего s.

Пусть $v_s(L) = |L \cap B_N^s|$ и $v_{\leqslant s}(L) = |L \cap B_N^{\leqslant s}|$ — соответственно количество векторов веса s и количество векторов веса не больше s в линейном подпространстве $L \subset B_N$; набор $\{v_s(L)\}_{s=0}^N$ называют *весовым спектром* подпространства L.

Теорема 1. *Если L — случайное линейное подпространство B_N, имеющее равновероятное распределение на множестве всех его k-мерных подпространств, то при $s = 1, 2, \ldots, N$*

$$\mathbf{E}\, v_s(L) = C_N^s \frac{2^k - 1}{2^N - 1}, \quad \mathbf{D}\, v_s(L) = C_N^s \frac{(2^k - 1)}{(2^N - 1)} \frac{(2^N - 2^k)}{(2^N - 2)} \left(1 - \frac{C_N^s}{2^N - 1}\right),$$

и при $s, t \in \{1, 2, \ldots, N\}$, $s \neq t$,

$$\mathrm{cov}\,(v_s(L), v_t(L)) = -C_N^s C_N^t \frac{(2^k - 1)(2^N - 2^k)}{(2^N - 1)^2 (2^N - 2)}.$$

Теорема 2. *При $s = 1, 2, \ldots, N$*

$$\mathbf{E}\, v_{\leqslant s}(L) = 1 + \frac{2^k - 1}{2^N - 1} \sum_{r=1}^{s} C_N^r,$$

$$\mathbf{D}\, v_{\leqslant s}(L) = \frac{(2^k - 1)}{(2^N - 1)} \frac{(2^N - 2^k)}{(2^N - 2)} \left(1 - \frac{1}{2^N - 1} \sum_{r=1}^{s} C_N^r\right) \sum_{r=1}^{s} C_N^r.$$

Следствие. *Пусть $\mu(L) = \min\{w(x)\colon\ x \in L \backslash \{0\}\}$ — минимальный вес ненулевого вектора в подпространстве L. Если L — случайное равновероятное k-мерное подпространство в B_N, то*

$$\left(1 + \frac{2^N - 2^k}{2^N - 2} \frac{1}{\mathbf{E}\, v_{\leqslant s}(L)}\right)^{-1} \leqslant \mathbf{P}\,\{\mu(L) \leqslant s\} \leqslant \mathbf{E}\, v_{\leqslant s}(L).$$

Предельные теоремы для случайных величин $v_s(L)$ доказаны в [2], а асимптотические соотношения для $\mu(L)$ приведены в [1].

Теорема 3. *Если* X *и* Y *— независимые случайные векторы из* B_N, *причем* X *имеет равномерное распределение на* B_N^s, *а* Y *имеет равномерное распределение на* B_N^t, *то при* $|s-t| \leqslant m \leqslant \min\{s+t, N\}$

$$\mathbf{P}\{w(X \oplus Y) = m\} = p^{(N)}(t,s,m) \stackrel{\text{def}}{=} \frac{C_s^{(t+s-m)/2} C_{N-s}^{(t-s+m)/2}}{C_N^t} \mathbf{I}\{m \equiv t+s \,(\mathrm{mod}\, 2)\},$$

$$\mathbf{E}\, w(X \oplus Y) = s + t - \frac{2st}{N}, \quad \mathbf{D}\, w(X \oplus Y) = 4\frac{s(N-s)t(N-t)}{N^2(N-1)}.$$

Для произвольных $X_1, X_2, \ldots, X_n \in B_N$ и любого $s \in \{0, 1, \ldots, N\}$ положим

$$v_s^*(X_1, X_2, \ldots, X_n) = \sum_{a_1, a_2, \ldots, a_n = 0}^{1} \mathbf{I}\Big\{ w\Big(\sum_{j=1}^{n} a_j X_j \Big) = s \Big\}.$$

Если векторы $X_1, X_2, \ldots, X_n \in B_N$ линейно независимы, то $\{v_s^*(X_1, X_2, \ldots, X_n)\}_{s=0}^N$ — весовой спектр порожденного ими линейного подпространства.

Теорема 4. *Если* $\{X_1, X_2, \ldots, X_n\}$ *— набор независимых случайных векторов из* B_N, *в котором* X_k *имеет равномерное распределение на множестве векторов с* $w(X_k) = s_k$, $k = 1, 2, \ldots, n$, *то вектор-столбец*

$$V_n \stackrel{\text{def}}{=} (\mathbf{E}\, v_0^*(X_1, X_2, \ldots, X_n), \mathbf{E}\, v_1^*(X_1, X_2, \ldots, X_n), \ldots, \mathbf{E}\, v_N^*(X_1, X_2, \ldots, X_n))^T$$

вычисляется по формуле $V_n = 2^n (P_{s_n})^T (P_{s_{n-1}})^T \cdots (P_{s_1})^T (1, 0, \ldots, 0)^T$, *где* $P_s = \|p^{(N)}(s,i,j)/2 + \delta_{i,j}/2\|_{i,j=0}^N$ *и* $\delta_{i,j}$ *— символ Кронекера.*

СПИСОК ЛИТЕРАТУРЫ

1. *Балакин Г. В.* Системы булевых уравнений с искаженной правой частью при ограничениях на значения неизвестных и ошибок. — Труды по дискретной математике, 2008, т. 11, в. 1, с. 5–17.
2. *Копытцев В. А.* О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц. — Дискретн. матем., 2002, т. 14, в. 4, с. 87–109.