УДК 519.212.2

# О РАСПРЕДЕЛЕНИЯХ ВЕСОВЫХ СПЕКТРОВ СЛУЧАЙНЫХ ЛИНЕЙНЫХ ДВОИЧНЫХ КОДОВ

А. М. Зубков, В. И. Круглов

Рассмотрим $N$-мерное линейное пространство $B_N = \mathrm{GF}(2)^N = \{X = (x_1, \ldots, x_N) : x_1, \ldots, x_N \in \mathrm{GF}(2)\}$. Под линейным кодом размерности $k$ понимается $k$-мерное подпространство $L \subset B_N$ (см. [1, 2]).

Весом $\mathrm{w}(X)$ двоичного вектора $X = (x_1, \ldots, x_N) \in B_N$ называется количество ненулевых координат в векторе $X$. Через $B_N^s$ и $B_N^{\leqslant s}$ будем обозначать соответственно множества векторов фиксированного веса $s$ и веса, не превосходящего $s$, в $B_N$ :

$$B_N^s = \{X \in B_N : \mathrm{w}(X) = s\}, \quad B_N^{\leqslant s} = \{X \in B_N : \mathrm{w}(X) \leqslant s\},$$

тогда $B_N = \bigsqcup_{s=0}^{N} B_N^s$.

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

**Теорема 1.** Если $L$ — случайный $k$-мерный код в $B_N$, имеющий равновероятное распределение на множестве всех таких кодов, то при $s = 1, \ldots, N$

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

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

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

**Теорема 2.** При $s = 1, \ldots, N$

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

**Следствие 1.** Если $L \subset B_N$ — случайное равновероятное $k$-мерное подпространство и $\mu(L) = \min\{\mathrm{w}(x) : x \in L \backslash \{0\}\}$, то

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

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

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

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

Теорему 3 можно использовать для вычисления моментов сумм

$$v_s^*(X_1,\dots,X_n) \stackrel{\text{def}}{=} \sum_{a_1,\dots,a_n=0}^{1} I\left\{\mathrm{w}\left(\sum_{j=1}^{n} a_j X_j\right) = s\right\}, s \in \{0,1,\dots,N\},$$

где $X_1, X_2, \dots, X_n \in B_N$ — независимые случайные векторы, распределения которых инвариантны относительно перестановок координат.

**Теорема 4.** Пусть $X_1,\dots,X_n$ — независимые случайные векторы, имеющие равномерное распределение на $B_N^s$, тогда

$$\mathbf{P}\{X_1,\dots,X_n \text{ линейно зависимы}\} \leqslant \frac{1}{2^N}\sum_{t=0}^{N} C_N^t \left[\left(1+\frac{c_{N,s,t}}{C_N^s}\right)^n - n\frac{c_{N,s,t}}{C_N^s} - 1\right],$$

где $c_{N,s,t} = \sum\limits_{j\geqslant 0}(-1)^j C_t^j C_{N-t}^{s-j}$.

## ЛИТЕРАТУРА


1. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.


УДК 519.7

# ОЦЕНКИ ЧИСЛА БУЛЕВЫХ ФУНКЦИЙ, ИМЕЮЩИХ АФФИННЫЕ И КВАДРАТИЧНЫЕ ПРИБЛИЖЕНИЯ ЗАДАННОЙ ТОЧНОСТИ[1]

А. М. Зубков, А. А. Серов[1]

Пусть $V_n = (\mathrm{GF}(2))^n$. Обозначим через $\mathbb{F}_2^{V_n}$ множество всех булевых функций и через $\mathbb{L}_n$, $\mathbb{A}_n$ и $\mathbb{Q}_n$ — множества всех линейных, аффинных и квадратичных функций от $n$ булевых аргументов соответственно; тогда $\mathbb{L}_n \subset \mathbb{A}_n \subset \mathbb{Q}_n$, $|\mathbb{L}_n| = 2^n$, $|\mathbb{A}_n| = 2^{n+1}$, $|\mathbb{Q}_n| = 2^{\binom{n}{2}+n+1}$.

Пусть $\rho(f,g) = |\{x \in V_n : f(x) \neq g(x)\}|$ — расстояние Хэмминга между булевыми функциями $f, g \in \mathbb{F}_2^{V_n}$ и $\rho(f,A) = \min\limits_{g\in A}\rho(f,g)$ для произвольных $f \in \mathbb{F}_2^{V_n}$ и $A \subset \mathbb{F}_2^{V_n}$. В [1–3] показано, что если $f \in \mathbb{F}_2^{V_n}$ — случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^{V_n}$, то для каждого фиксированного $x \in \mathbb{R}$

$$\lim_{n\to\infty}\mathbf{P}\left\{\frac{\rho(f,\mathbb{L}_n)-a_n}{b_n} < x\right\} = 1-e^{-e^x}, \quad \lim_{n\to\infty}\mathbf{P}\left\{\frac{\rho(f,\mathbb{A}_n)-a_n}{b_n} < x-\ln 2\right\} = 1-e^{-e^x},$$
$$\lim_{n\to\infty}\mathbf{P}\left\{\frac{\rho(f,\mathbb{Q}_n)-c_n}{d_n} < x\right\} = 1-e^{-e^x},$$

где

$$a_n = 2^{n-1} - 2^{\frac{n-1}{2}}\sqrt{n\ln 2}\left(1-\frac{\ln\ln 2^n + \ln 4\pi}{4n\ln 2}\right), \quad b_n = \frac{2^{\frac{n-1}{2}}}{2\sqrt{n\ln 2}},$$
$$c_n = 2^{n-1} - 2^{\frac{n-2}{2}}n\sqrt{\ln 2}\left\{1+\frac{1}{2n}-\frac{4\ln(\pi n^2\ln 2)-\ln 2}{8n^2\ln 2}\right\}, \quad d_n = \frac{2^{\frac{n-2}{2}}}{n\sqrt{\ln 2}}.$$

[1]Работа поддержана грантом РФФИ, проект № 11-01-00139.