ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 4
2014

А. М. Зубков, В. И. Круглов (Москва, МИ РАН)**. О весах векторов в случайных линейных пространствах над GF(p) .**

Зафиксируем простое число p и будем обозначать $\mathbf{F}_p^N = \{X = (x_1, x_2, \ldots, x_N) : x_1, x_2, \ldots, x_N \in \mathbf{F}_p\}$ линейное N-мерное пространство над простым полем $\mathbf{F}_p$. Под k-мерным линейным кодом будем понимать любое k-мерное ($k < N$) подпространство $L \subset \mathbf{F}_p^N$, а весом вектора $\mathbf{X} = (x_1, x_2, \ldots, x_N) \in \mathbf{F}_p^N$ будем называть число $w(\mathbf{X}) = \sum_{k=1}^N I\{x_k \neq 0\}$ его ненулевых координат.

Множество векторов фиксированного веса s в пространстве $\mathbf{F}_p^N$ будем обозначать через $(\mathbf{F}_p^N)_s$, а множество ненулевых векторов веса, не превосходящего s, будем обозначать через $(\mathbf{F}_p^N)_{\leqslant s}$:

$$(\mathbf{F}_p^N)_s = \{\mathbf{X} \in \mathbf{F}_p^N \mid w(\mathbf{X}) = s\}, \quad (\mathbf{F}_p^N)_{\leqslant s} = \{\mathbf{X} \in \mathbf{F}_p^N \mid 0 < w(\mathbf{X}) \leqslant s\};$$

при таких обозначениях $\mathbf{F}_p^N = \bigsqcup_{s=0}^N (\mathbf{F}_p^N)_s$.

О п р е д е л е н и е. Будем обозначать через $v_s(L) = |L \cap (\mathbf{F}_p^N)_s|$ и $v_{\leqslant s}(L) = |L \cap (\mathbf{F}_p^N)_{\leqslant s}|$ соответственно количество векторов веса s и количество ненулевых векторов веса не больше s в линейном коде L; набор $\{v_s(L)\}_{s=0}^N$ называют весовым спектром кода L .

Предельные пуассоновские теоремы для случайных величин $v_s(L)$ и аналогичных им доказывались в [2], [3].

Зафиксируем некоторый k-мерный линейный код L и будем рассматривать k^*-мерный случайный код L^* , выбираемый случайно и равновероятно из множества всех k^*-мерных подкодов кода L . Пусть $\{v_s(L^*)\}_{s=0}^N$ — весовой спектр выбранного случайного кода L^*.

Теорема 1. *Пусть $L \subset \mathbf{F}_p^N$ есть линейный k-мерный код в $\mathbf{F}_p^N$, имеющий весовой спектр $\{v_s = v_s(L)\}_{s=0}^N$, пусть L^* — случайный равновероятный k^*-мерный подкод L, $1 \leqslant k^* < k < N$. Тогда при $s = 1, 2, \ldots, N$*

$$\mathbf{E}\, v_s(L^*) = v_s(L)\frac{p^{k^*} - 1}{p^k - 1},$$

$$\mathbf{D}\, v_s(L^*) = v_s(L)\frac{(p^{k^*} - 1)(p^k - p^{k^*})(p - 1)}{(p^k - 1)^2}\left(1 - \frac{v_s(L) - (p - 1)}{p^k - p}\right)$$

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

$$\operatorname{cov}(v_s(L^*), v_t(L^*)) = -v_s(L)v_t(L)\frac{(p^{k^*} - 1)(p^k - p^{k^*})(p - 1)}{(p^k - 1)^2(p^k - p)}.$$

Теорема 2. *В условиях теоремы* 1

$$\mathbf{E}\, v_{\leqslant s}(L^*) = \frac{p^{k^*}-1}{p^k-1}\, v_{\leqslant s}(L),$$
$$\mathbf{D}\, v_{\leqslant s}(L^*) = \frac{(p^{k^*}-1)(p^k-p^{k^*})(p-1)}{(p^k-1)^2}\,\frac{p^k-1-v_{\leqslant s}(L)}{p^k-p}\, v_{\leqslant s}(L) \leqslant$$
$$\leqslant (p-1)\,\frac{p^k-p^{k^*}}{p^k-1}\,\mathbf{E}\, v_{\leqslant s}(L^*)$$

и для минимального веса $\mu(L^*) = \min\{w(\mathbf{X}) : \mathbf{X} \in L^*\backslash\{0\}\}$ *ненулевых векторов в подкоде* L^* *имеет место неравенство*

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

Теорема 3. *Пусть* $\mathbf{X}$ *и* $\mathbf{Y}$ *— независимые случайные векторы, пусть вектор* $\mathbf{X}$ *имеет равномерное распределение на множестве* $(\mathbf{F}_p^N)_s$ *всех векторов веса* s*, а вектор* $\mathbf{Y}$ *имеет равномерное распределение на множестве* $(\mathbf{F}_p^N)_t$ *всех векторов веса* t*. Тогда для любого* m*, где* $|s-t| \leqslant m \leqslant \min\{s+t, N\}$*,*

$$\mathbf{P}\{w(\mathbf{X}+\mathbf{Y})=m\} = \sum_{j=\max\{0,s+t-N\}}^{s} \frac{C_s^j C_{N-s}^{t-j}}{C_N^t}\, C_j^{m-(s+t-2j)}\,\frac{(p-2)^{m-(s+t-2j)}}{(p-1)^j}$$

и

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

Эти результаты могут применяться при исследовании системы шифрования Мак-Элис ([4], [5]). Доказательства теорем 1–3 опубликованы в [1].

СПИСОК ЛИТЕРАТУРЫ

1. *Зубков А. М., Круглов В. И.* Статистические характеристики весовых спектров случайных линейных кодов над GF(p). — Матем. вопросы криптографии, 2014, т. 5, в. 1, с. 27–38.
2. *Копытцев В. А., Михайлов В. Г.* Теоремы пуассоновского типа для числа специальных решений случайного линейного включения. — Дискретн. матем., 2010, т. 22, в. 2, с. 3–21.
3. *Михайлов В. Г.* Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество. — Дискретн. матем., 2007, т. 19, в. 1, с. 17–26.
4. *Berson T.* Failure of the McEliece public-key cryptosystem under message-resend and related-message attack. — Lect. Notes Comput. Sci., 1997, v. 1294, p. 213–220.
5. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory. — Jet Propulsion Lab. DSN, 1978, Progress Report 42–44.