WEIGHT SPECTRA OF RANDOM LINEAR CODES

A.M. Zubkov, V.I. Kruglov
Steklov Mathematical Institute, Russian Academy of Sciences
Moscow, RUSSIA
e-mail: zubkov@mi.ras.ru, kruglov@mi.ras.ru

Abstract

Weight spectra of random equiprobable linear codes over $GF(p)$ are concerned. For a random linear code over $GF(p)$ we derive explicit formulae for expectation and variance of number of vectors with fixed weight; bounds of the distribution of minimal weight of non-zero vectors are also obtained.

1 Introduction

Let p be a fixed prime number. By $\mathbf{F}_p^N = \{X = (x_1, \ldots, x_N) : x_1, \ldots, x_N \in \mathbf{F}_p\}$ we denote linear N-dimensional space over $\mathbf{F}_p$, a k-dimensional linear code is a k-dimensional subspace $L \subset \mathbf{F}_p^N$.

For a vector $X = (x_1, \ldots, x_N) \in \mathbf{F}_p^N$ the weight of X is the number

$$w(X) = \sum\nolimits_{i=1}^{N} I\{x_i \neq 0\}$$

of non-zero coordinates of X.

By $\left(\mathbf{F}_p^N\right)_s$ and $\left(\mathbf{F}_p^N\right)_{\leq s}$ we denote respectively the set of vectors in $\mathbf{F}_p^N$ having fixed weight s and the set of non-zero vectors of the weight less then or equal to s:

$$\left(\mathbf{F}_p^N\right)_s = \left\{X \in \mathbf{F}_p^N \,|\, w(X) = s\right\}, \quad \left(\mathbf{F}_p^N\right)_{\leq s} = \left\{X \in \mathbf{F}_p^N \,|\, 0 < w(X) \leq s\right\},$$

so $\mathbf{F}_p^N = \bigsqcup_{s=0}^{N} \left(\mathbf{F}_p^N\right)_s$.

Assume $v_s(L) = |L \cap \left(\mathbf{F}_p^N\right)_s|$ and $v_{\leq s}(L) = |L \cap \left(\mathbf{F}_p^N\right)_{\leq s}|$, the set $\{v_s(L)\}_{s=0}^N$ is called the weight spectrum of the code L.

2 Expectation and variance of $v_s(L)$ and $v_{\leq s}(L)$

Consider the set of all k-dimensional codes over $\mathbf{F}_p^N$. We refer to a code L having an equiprobable distribution on the set of all such codes as an equiprobable k-dimensional code over $\mathbf{F}_p^N$.

Theorem 1. *If L is an equiprobable k-dimensional code over $\mathbf{F}_p^N$, then for $s = 1, \ldots, N$*

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

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

and for $s,t \in \{1,\dots,N\}$, $s \neq t$,

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

Theorem 2. *If L is an equiprobable k-dimensional code over $\mathbf{F}_p^N$, then for $s = 1,\dots,N$*

$$\mathbf{E}v_{\le s}(L) = \frac{p^k-1}{p^N-1}\sum\nolimits_{r=1}^{s}(p-1)^r C_N^r,$$

$$\mathbf{D}v_{\le s}(L) = \frac{(p^k-1)(p^N-p^k)}{(p^N-1)^2}\sum\nolimits_{r=1}^{s}(p-1)^r C_N^r \times$$

$$\times\left(\left(1+\frac{1}{p^N-p}\right)(p-1) - \frac{1}{p^N-p}\sum\nolimits_{r=1}^{s}(p-1)^r C_N^r\right) \le$$

$$\le (p-1)\,\frac{p^N-p^k}{p^N-1}\,\mathbf{E}v_{\le s}(L).$$

Corollary 1. *If L is an equiprobable k-dimensional code over $\mathbf{F}_p^N$ and*

$$\mu(L) = \min\{w(x) :\, x \in L\backslash\{0\}\},$$

then

$$\frac{1}{1+\frac{p^N-p^k}{p^N-1}\,(p-1)(\mathbf{E}v_{\le s}(L))^{-1}} \le \mathbf{P}\{\mu(L) \le s\} \le \mathbf{E}v_{\le s}(L).$$

3 Distributions of sums of vectors with fixed weihgts

Theorem 3. *If X and Y are independent random vectors in $\mathbf{F}_p^N$, the vector X is uniformly distributed on the set of vectors of weight s and the vector Y is uniformly distributed on the set of vectors of weight t, then for $|s-t| \le m \le \min\{s+t, N\}$*

$$\mathbf{P}\{w(X+Y) = m\} = p^N(t,s,m) \stackrel{def}{=}$$

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

and

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

$$= \frac{st}{N}\left(\frac{4}{p-1}\frac{(N-s)(N-t)}{N(N-1)} + \frac{p-2}{p-1} + \left(\frac{p-2}{p-1}\right)^2 \frac{st-sN-tN+N}{N(N-1)}\right).$$

For any $X_1, \dots, X_n \in \mathbf{F}_p^N$ and any $s \in \{0, 1, \dots, N\}$ assume

$$v_s^*(X_1, \dots, X_n) = \sum_{a_1, \dots, a_n = 0}^{1} I\left\{w\left(\sum\nolimits_{j=1}^{n} a_j X_j\right) = s\right\}.$$

If vectors $X_1, \dots, X_n \in \mathbf{F}_p^N$ are linearly independent, then the set $\{v_s^*(X_1, \dots, X_n)\}_{s=0}^N$ is the weight spectrum of the linear subspace which has $X_1, \dots, X_n$ for its basis.

Theorem 4. *If $\{X_1, \dots, X_n\}$ are independent random vectors in $\mathbf{F}_p^N$ and X_k has equiprobable distribution on the set of vectors with weight $w(X_k) = s_k$, $k = 1, \dots, n$, then for vector-column*

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

we have

$$V_n = 2^n \left(P_{s_n}\right)^{\mathrm{T}} \left(P_{s_{n-1}}\right)^{\mathrm{T}} \dots \left(P_{s_1}\right)^{\mathrm{T}} (1, 0, \dots, 0)^{\mathrm{T}},$$

where $P_s = \left\| \frac{1}{2}\, p^N(s, i, j) + \frac{1}{2}\, \delta_{i,j} \right\|_{i,j=0}^{N}$ and $\delta_{i,j}$ — Kroneker delta.

References

[1] Balakin G.V. (2008). Systems of Boolean equations with distorded right part and bounds on values of variables and errors (in Russian). *Trudy po diskretnoi matematike*. Vol. **11**, Vol. 1, pp. 5-17.

[2] Kopytcev V.A. (2002). On the number of solutions of systems of Boolean equations in the set of vectors, having a fixed number of 1 (in Russian). *Diskretnaya Matematika*. Vol. **14**, Vol. 4, pp. 87-109.