*Seventh International Workshop on Optimal Codes and Related Topics*
*September 6-12, 2013, Albena, Bulgaria* *pp. 164-169*

# On asymptotic behavior of entropy of ellipsoids in a Hamming space [1]

Viacheslav Prelov prelov@iitp.ru
Kharkevich Institute for Information Transmission Problems,
Russian Academy of Sciences, Moscow, RUSSIA

**Dedicated to the memory of Professor Stefan Dodunekov**

**Abstract.** Asymptotic behavior of the entropy of an ellipsoid in a Hamming space of a growing dimension is investigated in the case where coefficients of the ellipsoid are monotone sequences of real numbers.

## 1 Introduction

Recall that an ellipsoid $E^n$ in the $n$-dimensional Hamming space $\mathbb{E}^n = \{0,1\}^n$ is defined as the set of binary vectors $x = (x_1, \ldots, x_n)$ of length $n$ that satisfy the inequality $\sum_{i=1}^{n} a_i x_i \le r$, i.e.,

$$E^n = \left\{ (x_1, \ldots, x_n) \;\Big|\; \sum_{i=1}^{n} a_i x_i \le r \right\},$$

where $r > 0$, $a_i$, $i = 1, \ldots, n$, are some nonnegative real numbers; and $x_i$, $i = 1, \ldots, n$, take values 0 or 1 . The term *ellipsoid* for $E^n$ is explained by the reason that in the considered case of a Hamming space the inequalities $\sum_{i=1}^{n} a_i x_i \le r$ and $\sum_{i=1}^{n} a_i x_i^2 \le r$ are equivalent. The entropy $H(E^n)$ of an ellipsoid $E^n$ is defined as $H(E^n) = \log |E^n|$, where $|E^n|$ is the cardinality (the number of elements) of the set $E^n$; here and in what follows, log denotes logarithm to the base 2.

In [1], Pinsker showed that for an arbitrary sequence of ellipsoids $E^n$, $n = 1, 2, \ldots$, in the case where coefficients $a_i = a_i(n)$ and $r = r(n)$ may depend on $n$, the equality

$$H(E^n) = \mathcal{H}_n(1 + o(1)), \quad n \to \infty, \tag{1}$$

[1] This research is partially supported by the Russian Foundation for Basic Research (project no. 12-01-00905-a)

holds if

$$\frac{\mathcal{H}_n}{\log n} \to \infty, \quad n \to \infty, \tag{2}$$

where

$$\mathcal{H}_n = \max \sum_{i=1}^{n} h(p_i); \tag{3}$$

$h(p) = -p \log p - (1-p) \log(1-p)$ is the binary entropy function, and the maximum in (3) is over all collections $P = (p_1, \ldots, p_n)$ such that $0 \le p_1, \ldots, p_n \le 1/2$ and $\sum\limits_{i=1}^{n} a_i p_i \le r(n)$.

In the general case, no explicit expressions (in terms of coefficients $a_i$ and $r$) for $\mathcal{H}_n$ nor explicit conditions for fulfilment of (2) have been obtained from (3). Our main goal is to obtain some explicit expressions for the principal term of the asymptotics for the entropy of ellipsoids as $n \to \infty$ for various behaviors of their coefficients in a special case where coefficients of ellipsoids are some fixed infinite sequences of real numbers.

## 2 Main results

We consider sequences of ellipsoids

$$E^n_{\mathbf{a},\mathbf{r}} = \left\{ (x_1, \ldots, x_n) \;\Big|\; \sum_{i=1}^{n} a_i x_i \le r_n \right\}, \quad n = 1, 2, \ldots, \tag{4}$$

where $\mathbf{a} = (a_1, a_2, \ldots)$ and $\mathbf{r} = (r_1, r_2, \ldots)$ are some fixed sequences of positive real numbers. Moreover, we always assume that the sequence $\mathbf{r} = \{r_n\}$ does not decrease, i.e., $0 < r_1 \le r_2 \le \ldots$, and the sequence $\mathbf{a} = \{a_n\}$ is monotone: it either does not increase or does not decrease.

First note that in the special case where $\lim\limits_{n\to\infty} a_n = a$, $0 \le a < \infty$, the coefficients $a_n$ become equalized as $n \to \infty$, and the ellipsoids (4) become more and more similar to balls in the Hamming space; therefore, the entropy of an ellipsoid $E^n_{\mathbf{a},\mathbf{r}}$ becomes approximately equal to the entropy of a ball of radius $\dfrac{r_n}{a_n}$. In some cases, this simple reasoning allows us to exactly write out the principal term of the asymptotics for the entropy of ellipsoids $E^n_{\mathbf{a},\mathbf{r}}$. However, in other cases, and in particular in the cases where $a_n$ polynomially decreases to 0 as $n \to \infty$, this reasoning is rather rough, and the asymptotics for the entropy of ellipsoids $E^n_{\mathbf{a},\mathbf{r}}$ does not coincide with that of balls of radii $\dfrac{r_n}{a_n}$. Moreover, this reasoning does not apply to the case where $a_n \to \infty$ as $n \to \infty$. Our aim is

to find some conditions on the behavior of the coefficients $\{a_n\}$ and $\{r_n\}$ under which either the first or second of the above situation appears and to investigate the asymptotics for the entropy of ellipsoids if the second case occurs.

In the first theorem, some conditions are given for relation (2) to be fulfilled or not.

**Theorem 1.** (i) *If the sequence $\{a_n\}$ does not increase and the sequence $\{r_n\}$ does not decrease, then Pinsker's condition* (2) *is fulfilled if and only if the equality*

$$\lim_{n\to\infty} \frac{a_n}{r_n} = 0. \tag{5}$$

*holds.*

(ii) *If the sequences $\{a_n\}$ and $\{r_n\}$ do not decrease, then* (2) *is fulfilled if at least one of the following conditions is valid:*

a) *There exists $\gamma$, $0 < \gamma \le 1$, such that* [2] $\lim\limits_{n\to\infty} \dfrac{a_{n^\gamma}}{r_n} = 0$*;*

b) *There exist some constants $c_1 > 0$, $c_2 > 0$, $s > 1$, and $t > 1$ such that $a_n \le c_1 \log^s n$ and $r_n \ge c_2 \log^t n$ for all sufficiently large $n$.*

(iii) *If the sequences $\{a_n\}$ and $\{r_n\}$ do not decrease, then* (2) *is not fulfilled* (*i.e., $\mathcal{H}_n \le C \log n$, where $C$ is a positive constant*) *if $\liminf\limits_{n\to\infty} \dfrac{a_n}{r_n} > 0$ and at least one of the following conditions is valid:*

a) $\lim\limits_{n\to\infty} a_n < \infty$*;*

b) $a_n \sim \log^s n$, $n \to \infty$, *where* $0 < s \le 1$*;*

c) $a_n \sim \underbrace{\log\log\ldots\log}_{k} n$, $n \to \infty$, *where $k \ge 1$ is an arbitrary integer.*

As can be seen from Theorem 1, in the case where the sequence $\{a_n\}$ does not decrease, a necessary and sufficient condition for validity Pinsker's condition (2) cannot be obtained without extra assumptions. The case of a nondecreasing sequence $\{a_n\}$ is rather difficult for investigation. If follows from the second claim of Theorem 1 that the entropy of an ellipsoid can increase faster than $\log n$ even in the case where the sequence $r_n$ increases substantially slower than $a_n$: for example, $a_n$ can increase as $n^s$ and $r_n$ as $n^t$, where $s > t > 0$; or $a_n$ can increase as $\log^s n$ and $r_n$ as $\log^t n$ where $s > t > 1$. Moreover, if $a_n = 2^n$ and $r_n = 2^n - 1$, then this ellipsoid coincides with the whole space $\mathbb{E}^{n-1}$ in spite of the fact that $r_n < a_n$ for all $n$. On the other hand, it follows from third claim of

[2] If $n^\gamma$ is not an integer, then by definition we set $a_{n^\gamma} = a_{\lfloor n^\gamma \rfloor}$ where $\lfloor x \rfloor$ is the maximum integer smaller or equal to $x$. A similar agreement relates to other subsequences of integers which occur below.

Theorem 1 that Pinsker's condition is not fulfilled ( i.e., $\mathcal{H}_n \le C \log n$) in many cases where the sequence $\{a_n\}$ increases no faster than $\log n$ and $\liminf\limits_{n\to\infty} \dfrac{a_n}{r_n} > 0$.

Now note that in the case where the sequence $\{a_n\}$ does not decrease and $\dfrac{a_n}{r_n} \to 0$ as $n \to \infty$, the following statement is valid.

**Proposition 1.** *Assume that a sequence* $\{a_n\}$ *does not decrease,* $\lim\limits_{n\to\infty} a_n = a < \infty$, *and* $r_n \to \infty$ *as* $n \to \infty$.

- *If* $\lim\limits_{n\to\infty} \dfrac{r_n}{n} = t > 0$, *where* $t$ *can also be equal to infinity, then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = n\overline{h}(t/a)(1 + o(1)), \quad n \to \infty, \tag{6}$$

*where*

$$\overline{h}(x) = \begin{cases} h(x) & \text{if} \quad 0 \le x \le 1/2, \\ 1 & \text{if} \quad x \ge 1/2. \end{cases} \tag{7}$$

- *If* $\lim\limits_{n\to\infty} \dfrac{r_n}{n} = 0$, *then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = \left(\frac{r_n}{a} \log \frac{n}{r_n}\right)(1 + o(1)), \quad n \to \infty. \tag{8}$$

The proof of this proposition is based on the fact that the ellipsoid $E^n_{\mathbf{a},\mathbf{r}}$ contains a ball of radius $\dfrac{r_n}{a_n}$ and

$$E^n_{\mathbf{a},\mathbf{r}} \subseteq \mathbb{E}^k \times B^{n-k}\left(\frac{r_n}{a_n}\right),$$

where $\mathbb{E}^k$ is a $k$-dimensional Hamming space and $B^{n-k}\left(\dfrac{r_n}{a_n}\right)$ is a ball of radius $\dfrac{r_n}{a_n}$ in a Hamming space of dimension $(n-k)$, where $k = k(n) \to \infty$ sufficiently slowly so that $\dfrac{k}{n} \to 0$ and $k = o\left(r_n \log \dfrac{n}{r_n}\right)$.

To state the next proposition, we need some definitions.

A sequence $\{x_n\}$ is said to be *regular* if for any monotone increasing sequence $\{\delta_n\}$, $\delta_n \to 1$ as $n \to \infty$, there exists a finite or infinite limit $\lim\limits_{n\to\infty} \dfrac{x_n}{x_{n\delta(n)}}$.

Recall also that a sequence $\{\ell_n\}$ is said to be *slowly varying* if $\lim\limits_{n\to\infty} \dfrac{\ell_n}{\ell_{\lambda n}} = 1$ for any $\lambda > 0$; and a sequence $\{y_n\}$ is said to be *tame-varying* if $y_n = \dfrac{\ell_n}{n^\alpha}$ where $\alpha > 0$ and $\{\ell_n\}$ is a slowly varying sequence.

**Proposition 2.** *Assume that a sequence* $\{a_n\}$ *does not increase and condition* (5) *is fulfilled. Then the following statements are valid:*

- *If* $\lim\limits_{n\to\infty} \dfrac{na_n}{r_n} = 0$, *then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = n(1+o(1)), \quad n \to \infty; \tag{9}$$

- *If* $\lim\limits_{n\to\infty} \dfrac{na_n}{r_n} = \infty$ *and* $\{\delta(n)\}$ *is any monotone sequence such that* $\delta(n) \to 1$ *and* $\log(1-\delta(n)) = o\left(\log \dfrac{na_n}{r_n}\right)$ *as* $n \to \infty$, *then*

$$\left(\frac{r_n}{a_{n\delta(n)}} \log \frac{na_n}{r_n}\right)(1+o(1)) \le H(E^n_{\mathbf{a},\mathbf{r}}) \le \left(\frac{r_n}{a_n} \log \frac{na_n}{r_n}\right)(1+o(1)), \quad n \to \infty. \tag{10}$$

*Moreover, if the sequence* $\{a_n\}$ *is regular, then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = \left(\frac{r_n}{a_n} \log \frac{na_n}{r_n}\right)(1+o(1)), \quad n \to \infty, \tag{11}$$

*and if the sequence* $\{a_n\}$ *is irregular, then equality* (11) *holds for some subsequence* $n_k \to \infty$ *as* $k \to \infty$*;*

- *If* $\lim\limits_{n\to\infty} \dfrac{r_n}{na_n} = c$, $0 < c < \infty$, *then the following inequalities are valid:*

$$\frac{2c}{1+2c}\, n(1+o(1)) \le H(E^n_{\mathbf{a},\mathbf{r}}) \le \overline{h}(c) n(1+o(1)), \quad n \to \infty. \tag{12}$$

*Moreover, if* $\{a_n\}$ *is a slowly varying monotone sequence, then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = \overline{h}(c) n(1+o(1)), \quad n \to \infty, \tag{13}$$

*and if* $\{a_n\}$ *is a monotone tame-varying sequence such that* $a_n = \dfrac{\ell_n}{n^\alpha}$, $0 < \alpha \le 1$, *where* $\{\ell_n\}$ *is a slowly varying sequence, then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) \ge \max_\gamma \left[\gamma \overline{h}\left(\frac{(1-\gamma)^\alpha c}{\gamma}\right)\right] n(1+o(1)) \ge \gamma_0 n(1+o(1)), \quad n \to \infty, \tag{14}$$

*where* $\gamma_0$ *is defined by the equation*

$$\gamma_0 = 2c(1-\gamma_0)^\alpha. \tag{15}$$

To find the principal term of the asymptotics for $H(E^n_{\mathbf{a},\mathbf{r}})$ as $n \to \infty$ in the case where $a_n \to \infty$ as well as in the case where $\{a_n\}$ does not increase (but is not slowly varying) and $\lim\limits_{n\to\infty} \dfrac{r_n}{na_n} = c,\ 0 < c < \infty$, we consider the most typical special case where the coefficients of an ellipsoid are polynomial functions of $n$. The corresponding statement is formulated in Theorem 2 below. A similar statement can be proved in some other cases of behavior of ellipsoid coefficients.

**Theorem 2.** (i) *Assume that* $\lim\limits_{n\to\infty} \dfrac{a_n}{n^\gamma} = 1$ *and* $\lim\limits_{n\to\infty} \dfrac{r_n}{n^\alpha} = c$, *where* $\gamma > 0,\ \alpha > 0$ *and* $c > 0$ *are some constants and* $\alpha < \gamma + 1$. *Then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = c^{1/(1+\gamma)}(\gamma+1)\left(\frac{I}{\gamma}\right)^{\gamma/(1+\gamma)} n^{\alpha/(1+\gamma)}(1+o(1)), \quad n \to \infty, \tag{16}$$

*where*

$$I = \int\limits_0^\infty \frac{t^{1/\gamma}\,dt}{1+2^t}; \tag{17}$$

(ii) *Assume that* $\lim\limits_{n\to\infty} \left(a_n n^{1-\sigma}\right) = 1$ *and* $\lim\limits_{n\to\infty} \dfrac{r_n}{na_n} = c$, *where* $0 \le \sigma < 1,\ c > 0$ *and* $2c\sigma < 1$. *Then*

$$H(E^n_{\mathbf{a},\mathbf{r}}) = \left[c\sigma\mu + \log\left(1+2^{-\mu}\right)\right] n(1+o(1)), \quad n \to \infty, \tag{18}$$

*where* $\mu$ *is a solution of the equation*

$$\mu^{\sigma/(1-\sigma)} \int\limits_\mu^\infty \frac{dt}{t^{1/(1-\sigma)}(1+2^t)} = c(1-\sigma). \tag{19}$$

Proofs of these and some other statements can be found in [2].

## References

[1] M. S. Pinsker, Entropy of an Ellipsoid in a Hamming Space, *Probl. Peredachi Inf.*, **36** (4), 2000, 47-52.

[2] V. V. Prelov, On computation of entropy of an ellipsoid in a Hamming space, *Probl. Peredachi Inf.*, **49** (1), 2013, 3-18.