Introduction. The measure of indeterminity was considered by R. V. L. Hartley in 1923, [Har], later C. Shannon

Remark on the Entropy of Arithmetic functions

Milan Paštéka
Pedagogická fakulta Trnavskej Univerzity
Priemyselná 4, P.O. BOX 4, Sk-914 43, Trnava,SR
e-mail: pasteka...mat.savba.sk

SUMMARY.*In the present paper the definition of the entropy of arithmetic functions, based on the classical definition of entropy is given. Two properties of this notion are proved*

Introduction. The measure of indeterminacy was considered by R. V. L. Hartley in 1923, [Har], later C. Shannon introduced for this value the name *entropy of experiment* or *entropy of random variable*, [Sh1] [Sh2]. If η is a random variable with possible results $a_1, ..., a_k$ then *entropy* of η is defined as

(i) $$H(\eta) = -(P(\eta = a_1)\log P(\eta = a_1) + ... + P(\eta = a_k)\log P(\eta = a_k)).$$

This value is always nonnegative, convexity of the function $x \log x$ provides that the maximum of $H(\eta)$ is $\log k$, in the case $P(\eta = a_j) = \frac{1}{k}$. And $H(\eta) = 0$ only in the case $P(\eta = a_j) = 1$ for some j. Later there were given some axiomatic definitions of entropy, which lead to formula (i). We refer to the paper [Fad], or to the monography [J-J].

Formulation. The formula (i) will be the starting point for our considerations. Denote by $\mathbf{N}$ the set of positive integers, $\mathbf{C}$ the set of complex numbers and $\mathbf{R}$ the set of real numbers. If $A \subset \mathbf{N}$ then put

$$\gamma_N(A) = \frac{|A \cap [1, N]|}{N}.$$

If $\mathcal{P}$ is a property then instead of $\gamma_N(\{n; \mathcal{P}(n)\})$ we shall write only $\gamma_N(\mathcal{P})$. Notice that if it exists the limit $\lim_{N\to\infty} \gamma_N(A) := \gamma(A)$ then the value $\gamma(A)$ is called the asymptotic density of A. Also in this case we shall write $\gamma(\mathcal{P})$ instead of $\gamma(\{n; \mathcal{P}(n)\})$.

Let $f : \mathbf{N} \to \mathbf{X}$ be an arithmetic function where $\mathbf{X}$ is a compact metric space. Consider $\mathcal{D} = \{C_1, ..., C_k\}$ a system of subsets of $\mathbf{X}$. Put

$$H(f, \mathcal{D}, N) := -\sum_{j=1}^{k} \gamma_N(f \in C_j) \log \gamma_N(f \in C_j)$$

for $N \in \mathbf{N}$. If there exists a limit

$$H(f, \mathcal{D}) := \lim_{N\to\infty} H(f, \mathcal{D}, N)$$

then this value will be called the *asymptotic entropy of* f *with respect to* $\mathcal{D}$.

Remark that this limit exists always in the case if the sets $f^{-1}(C_j)$ for $j = 1, ..., k$ have the asymptotic density. (As usually we put $0 \cdot \log 0 = 0$). In the case when f is a real valued additive arithmetic function, so that the series $\sum \frac{||f(p)||}{p}, \sum \frac{||f(p)||^2}{p}$ ($p-$ prime), converge, then the result of Erdös and Wintner (see for instance[E]) guaranties that the value $H(f, \mathcal{D})$ exists in the case if $\mathcal{D}$ contains only intervals.

Denote for $z \in \mathbf{X}, \varepsilon > 0$ by $B(z, \varepsilon)$ the open ball with the centre z and the radius ε.

Let us consider $\mathcal{D} = \{B_1, ..., B_k\}$ as a cover of closure of the range of f by open balls. Remark that this closure is a compact set, thus such a cover always exists. Thus we can put in the usual way $n(\mathcal{D}) = max\{diam B_j; j = 1, ..., k\}$. Thus we can define the value

$$H(f, \varepsilon) = \inf\{H(f, \mathcal{D}); n(\mathcal{D}) < \varepsilon\}$$

for $\varepsilon > 0$. The limit

$$\lim_{\varepsilon \to 0+} H(f, \varepsilon) := H(f)$$

always exists and this value will be called *asymptotic entropy of* f. If $H(f) < \infty$ then we say that f has a finite asymptotic entropy.

Example 1. Let f be a periodic function modulo m. Suppose that all the values $f(1), ..., f(m)$ are different. Thus we can consider a cover of its range $\mathcal{D} = \{B_1, ..., B_m\}$ such that $f(j) \in B_j$. We can suppose that the balls B_j are disjoint, thus

$$H(f, \mathcal{D}, N) \to -\sum_{j=1}^{m} \frac{1}{m} \log \frac{1}{m} = \log m$$

and so $H(f) = \log m$. Similarly it can be proved that $\mathcal{H}(f) = \log m$.

Proposition 1. Let $f : \mathbf{N} \to \mathbf{X}$ be such an arithmetical function that we have a disjoint decomposition

$$\mathbf{N} = A_1 \cup ... \cup A_m \cup R$$

where $\gamma(R) = 0$ and $\gamma(A_j)$ exists for $j = 1, ..., m$, and $\lim_{n \in A_j, n \to \infty} f(n) = L_j$, for $j = 1, ..., m$, and all these limits are different. Then

$$H(f) = -\sum_{j=1}^{m} \gamma(A_j) \log \gamma(A_j).$$

Proof. Let $\mathcal{D} = \{B_1, ..., B_k\}$ be a cover of the closure of range of f by open balls. Thus we have that $L_j \in B_{h_j}$, for $j = 1, ..., k$. If we suppose that $n(\mathcal{D}) < \varepsilon$ for a suitable $\varepsilon > 0$ then the sets B_{h_j} are different, moreover we can suppose the ball B_h for $h \neq h_j, j = 1, ..., m$ contains only the elements $f(n)$ for $n \in R$ with exclusion at most a finite number of n. This $\gamma_N(B_h) \to 0$ for $h \neq h_j, j = 1, ..., m$, and $\gamma_N(B_{h_j}) \to \gamma(A_j)$ as $N \to \infty$. Then the assertion follows.

Proposition 2. Let $f : \mathbf{N} \to [0, 1]$ be an arithmetical function, with a continuous asymptotic distribution function. Then $H(f) = \infty$.

Proof. Consider $\mathcal{D} = \{I_1, ..., I_k\}$ as a cover the unit interval by the system of open intervals. Denote by g the asymptotic distribution function of f. If $I_j = (x_1^{(j)}, x_2^{(j)})$, such that $x_1^{(j)} < x_1^{(j+1)} < 1$ then $\gamma(f \in I_j) = g(x_2^{(j)}) - g(x_1^{(j)}) := h_j$, as

$j = 2, ..., k-1$ and $\gamma(f \in I_1) = g(x_2^{(1)}) := h_1$ and $\gamma(f \in I_k) = 1 - g(x_1^{(k)}) := h_k$. Thus we have

$$H(f, \mathcal{D}) = \sum_{j=1}^{k} h_j \log \frac{1}{h_j}. \tag{1}$$

The intervals $I_j, j = 1, ..., k$ cover the unit interval and so the sum of its Riemann - Stieltjes measures is bigger than 1, thus $\sum_{j=1}^{k} h_j \geq 1$. The function g is uniformly continuos on $[0, 1]$, thus there exists such $\varepsilon > 0$ that for $n(\mathcal{D}) < \varepsilon$ it holds $\frac{1}{h_j} > m$ for m positive integer - fixed. Therefore (1) implies $H(f, \varepsilon) > logm$, and for $m \to \infty$ we obtain the assertion.

References

[Fad] Fadejev, D. K. : To notion of entropy of a finitee probability scheme, (in Russian), Usp. Mat. Nauk 11 (1956), 227 - 231

[E] Elliott, P.D.T.A.: Probabilistic Number Theory, Springer - Verlag, New York, Heidelberg, Berlin, 1979

[Har] Hartley, R. V. L. : Transmison of information. Bell Syst. Tech. J. 7, 1928, p. 535

[J-J] A. M. Jaglom, I. M. Jaglom : Probability and Information (in Russian), Gos. iz. fiz. mat. lit. Moscov, 1960

[Sh1] Shannon, C.: A mathematical theory of communication. Bell Syst. Tech. J. 27, 1948 p. 379

[Sh2] Shannon, C.: Certain results in coding theory for noisy channels, Inf. and Control 1, (1965) p. 390