The Entropy of a Natural Number

N. Minculete[1], C. Pozna[2,3]

[1]Departament of REI, University Dimitrie Cantemir of Braşov, Romania,
e-mail: minculeten@yahoo.com
[2]Department of Automation, Transilvania University of Brasov, Brasov, Romania
[3]Department of Informatics, Széchenyi István University, Győr, Hungary,
e-mail:pozna@sze.hu

Abstract: The aim of this paper is to introduce the concept of the entropy of a natural number. This new concept is the synthesis of the entropy and of the prime numbers concepts. The natural number structure is represented by its factorization in prime numbers. The entropy gives us the possibility to analyze the order of this structure. Using the natural number entropy concept has reviled interesting results concerning the internal structure of a natural number.

Keywords: Shannon's entropy, prime numbers, natural numbers

1. Introduction

Present paper proposes an original idea which corroborates two important concepts: the entropy and the natural numbers.

The entropy is defined, in information theory like a measure of uncertainty. For this reason it is associated with a random variable. The most acknowledged way to define the entropy is the Shannon entropy. The idea (inspired from thermodynamics) is to measure the uncertainty associated with the mentioned random variable. Thereby the Shannon entropy is the expected value of the information contained in a message [5]. The specific realization of the random variable is defined like message. The entropy is the minimum descriptive complexity of a random variable

A natural number is called a prime number if it is greater than 1 and has exact two divisors, one and the number itself. The fundamental theorem of arithmetic states that each natural number can be written as a product of prime numbers in a unique way. For this reason the primes can be considered the basic elements on which are constructed the natural numbers.

Each natural number can be expressed like a product of prime number (of basic elements). These prime numbers are prime factors of the number. Each prim number can have a certain multiplicity. The multiplicity of prime relative to a natural number is the largest exponent for which this prime divides the natural number.

If for a natural number we consider that a prime factor can be meet (found) with the frequency of its multiplicity we can define the relative frequency of the prime factor like the ratio between its multiplicity and the sum of the prim factors multiplicity.

The concept of relative frequency is related to the concept of probability. This gives us the possibility to define the entropy of a natural number.

Let $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r} > 1$ be a positive integer number, where p_i are the prime factors of the natural number and a_i is the multiplicity of the factor p_i.

If $\Omega(n) = a_1 + a_2 + ... + a_r$ is total number of prime factors of *n*, then we can define the probabilities $p(a_i) = \frac{a_i}{\Omega(n)}$, for every $i \in \{1, 2, ..., r\}$, so, we associate to *n* the random variable $X(n) = \{p(a_1), p(a_2), ..., p(a_r)\}$, where $\sum_{i=1}^{r} p(a_i) = 1$.

In section 2 we introduce the natural numbers entropy concept definition and we present several initial analyses of this concept. Section 3 will continue this analysis for special cases of natural numbers the *k* – free and the *k* – full numbers. In Section 4 we have analyzed the exponential divisors of a natural number from the point of view of the distance between two random variables. Conclusions will end the paper.

2. The definition and analysis of the natural number entropy

In this section we define the natural number entropy and based on this definition we analyze this concept from mathematical point of view. The mentioned analysis is focused in reveling particular values of entropy and in boundaries finding.

Definition 1. *The entropy of a positive integer number* $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r} > 1$ is given by

$$H(n) = -\sum_{i=1}^{r} p(a_i) \log p(a_i). \tag{1}$$

Since $0 \log 0 = 0$, by convention, we take $H(1) = 0$.

Relation (1) can be written in following way

$$H(n) = \log \Omega(n) - \frac{1}{\Omega(n)} \sum_{i=1}^{r} a_i \log a_i. \tag{2}$$

For example, if $n = 2 \cdot 3^2 \cdot 5^3$, then the entropy of *n* is

$$H(n) = \log 6 - \frac{1}{6}(2 \log 2 + 3 \log 3) = \frac{1}{6} \log \frac{6^6}{2^2 3^3} = \frac{1}{6} \log 2 \cdot 6^3 \approx 1.011.$$

Remark 1. From the previous definitions we can obtain the following results:

If $n = p^a$, then $H\left(p^a\right) = 0$.

If $n = p_1 p_2 ... p_r$, we obtain $H(n) = \log \omega(n)$, where $\omega(n)$ is the number of distinct prime factors of n;

If $n = \left(p_1 p_2 ... p_r\right)^k$, then $H(n) = \log \omega(n)$.

Theorem 2. For all $n \geq 2$, there we have:

$$0 \leq H(n) \leq \log \omega(n). \tag{3}$$

Proof. From (1), we have $H(n) = -\sum_{i=1}^{r} p(a_i) \log p(a_i)$, with $\sum_{i=1}^{r} p(a_i) = 1$, but $p(a_i) \log p(a_i) \leq 0$, therefore, we deduce $H(n) = -\sum_{i=1}^{r} p(a_i) \log p(a_i) \geq 0$. We consider the function $f : [1, \infty) \to R$, defined by $f(x) = x \log x$. But $f''(x) = \frac{1}{x} > 0$, which means that the function *f* is convex. Therefore, if we apply Jensen's inequality for the function *f*, then we deduce the inequality

$$\sum_{i=1}^{r} a_i \log a_i \geq r \frac{\sum_{i=1}^{r} a_i}{r} \log \frac{\sum_{i=1}^{r} a_i}{r} = \Omega(n) \log \frac{\Omega(n)}{\omega(n)}. \tag{4}$$

Combining relations (2) and (4), we find that $H(n) \leq \log \omega(n)$. Thus, the proof of theorem is complete.

Theorem 3. For all $n \geq 3$, we have:

$$0 \leq H(n) \leq \log \log n - \log \log \log n + \log c_1, \tag{5}$$

where $c_1 = 1.38402...$.

Proof. In [3], G. Robin proved that $\omega(n) \leq \frac{\log n}{\log \log n} c_1$, for all $n \geq 3$. Using this relation and relation (3), we obtain the relation desired.

We observe that the entropy of a positive integer number n is minimum (i.e. 0) when n is a prime number or a power of prime number, and the entropy is maximum (i.e. $\log \omega(n)$), when n is square-free or a square-free to power k, where $k \geq 2$.

3. Applications of the entropy for different types of the positive integer numbers

This section continues the analysis of natural number entropy considering special cases like *k* – free, *k* – full numbers or Mersenne number.

Using the concept of natural number entropy we have the following results:

For $n = p^a q^b$ and $m = p^b q^a$, we have $H(n) = H(m)$. This remark implies the following result: if $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ and $m = p_1^{a_{\sigma(1)}} p_2^{a_{\sigma(2)}} \ldots p_r^{a_{\sigma(r)}}$, then $H(n) = H(m)$, where $\sigma \in S_r$, and S_r is the symmetric group of degree r.

If n is a number k-free (see [4]), so $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, with $a_i \le k-1$, where $k \ge 2$, then using relation (2), we find that

$$\log \omega(n) \ge H(n) \ge \log \Omega(n) - \frac{\omega(n)}{\Omega(n)}(k-1)\log(k-1). \tag{6}$$

If n is a number k-full (see [4]), so $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, with $a_i \ge k$, where $k \ge 2$, then using relation (2), we find that

$$0 \le H(n) \le \log \Omega(n) - \frac{\omega(n)}{\Omega(n)} k \log k. \tag{7}$$

For a number 2-full, which is called and powerfull (see [4]), applying relation (7), we get the inequality

$$0 \le H(n) \le \log \Omega(n) - \frac{2\omega(n)\log 2}{\Omega(n)}. \tag{8}$$

We note by $\sigma(n)$ the sum of the positive divisors of n. From [4], if we have $\sigma(n) = 2n$, then, we say that n is a perfect number. Theorem Euler-Euclid (see [2]) show that every perfect number has the form $n_k = 2^k\left(2^{k+1}-1\right)$, where $2^{k+1}-1$ is a prime number and $k \ge 1$. Hence, we have $H(n) = \frac{k}{k+1}\log\frac{k+1}{k}$. Applying Lagrange's Theorem for the function $f(x) = \log x$ on $[k, k+1]$, we deduce the relation

$$\frac{1}{k+1} < \log(k+1) - \log k < \frac{1}{k},$$

which implies the inequality

$$k\log\left(\frac{k+1}{k}\right) < 1 < (k+1)\log\left(\frac{k+1}{k}\right).$$

Therefore, we obtain

$$\frac{1}{k+1} - \frac{1}{(k+1)^2} < H(n) < \frac{1}{k+1}. \tag{9}$$

It is known that the Mersenne numbers form is 2^k-1, then if $m_k=2^k-1$ is a prime, is called a prime Mersenne number. According with [2, 4] is not known if there are an infinity of this type numbers of number, but if we assume that there are an infinity then there are an infinity of perfect numbers $(n_k)_{k\geq 1}$, and using relation (9), we deduce the following result.

$$\lim_{k\to\infty} H(n_k)=0 \text{ and } \lim_{k\to\infty} kH(n_k)=1. \tag{10}$$

4. Kullback-leibler distance between two positive integer numbers

The entropy concept is used in several developments like the distance between two random variables or like the relative information between two distributions. Considering this developments it was very attractive to used them for the natural numbers entropy.

In [1] the relative entropy or (Kullback-Leibler distance) between two random variables $\mathbf{p}=\{p_1,p_2,...,p_r\}$ and $\mathbf{q}=\{q_1,q_2,...,q_r\}$ was introduced in the following way:

$$\mathrm{D}(\mathbf{p}\|\mathbf{q})=\sum_{i=1}^{r} p_i \log\frac{p_i}{q_i}. \tag{11}$$

We consider two positive integer numbers $n=p_1^{a_1}p_2^{a_2}...p_r^{a_r}$ and $m=q_1^{b_1}q_2^{b_2}...q_r^{b_r}$. From here, we define the probabilities $p(a_i)=\frac{a_i}{\Omega(n)}$ and $q(b_i)=\frac{b_i}{\Omega(m)}$, for every $i\in\{1,2,...,r\}$, so, we associate to n and m the random variables $X(n)=\{p(a_1),p(a_2),...,p(a_r)\}$ and $X(m)=\{q(b_1),q(b_2),...,q(b_r)\}$, where $\sum_{i=1}^{r}p(a_i)=1$ and $\sum_{i=1}^{r}q(b_i)=1$.

Similar with Kullback-Leibler distance between two random variables, we define the Kullback-Leibler distance between two positive integer numbers.

Definition 2. The Kullback-Leibler distance between two positive integer number n and m with $\omega(n)=\omega(m)$ and factorization thus $n=p_1^{a_1}p_2^{a_2}...p_r^{a_r}$ and $m=q_1^{b_1}q_2^{b_2}...q_r^{b_r}$ is given as

$$\mathrm{D}(n\|m)=\sum_{i=1}^{r} p(a_i)\log\frac{p(a_i)}{q(b_i)}. \tag{12}$$

Relation (12) can be written in following way

$$\mathrm{D}(n\|m)=\log\frac{\Omega(m)}{\Omega(n)}+\frac{1}{\Omega(n)}\sum_{i=1}^{r} a_i\log\frac{a_i}{b_i}. \tag{13}$$

For example, if $n=2\cdot 3^2\cdot 5^3$ and $m=3\cdot 5^2\cdot 7^4$, then the entropy relative of n and m is

$$D(n||m)=\log\frac{7}{6}+\frac{1}{2}\log\frac{3}{4}\approx 0.0103.$$

Remark 2. It is easy to see that $D(n||m)\neq D(m||n)$.

In [**6**], M. V. Subbarao was introduced the notion of exponential divisor. So if , we have a number $n=p_1^{a_1}p_2^{a_2}...p_r^{a_r}>1$, then the number $d=\prod_{i=1}^{r}p_i^{b_i}$, with $b_i\mid a_i$, for all $i=\overline{1,r}$, is called exponential divisor (or e-divisor). We note $d\mid_{(e)} n$. In this case, because $\omega(n)=\omega(d)$, we deduce

$$D(n||d)=\log\frac{\Omega(d)}{\Omega(n)}+\frac{1}{\Omega(n)}\sum_{i=1}^{r}a_i\log\frac{a_i}{b_i}. \tag{14}$$

For $\gamma(n)=p_1p_2...p_r$ which is the lowest divisor of *n*, we calculate the relative entropy between *n* and $\gamma(n)$ and we obtain

$$D(n||\gamma(n))=\log\frac{\omega(n)}{\Omega(n)}+\frac{1}{\Omega(n)}\sum_{i=1}^{r}a_i\log a_i. \tag{15}$$

From (14) and (15), we deduce the difference

$$D(n||d)-D(n||\gamma(n))=\log\frac{\Omega(d)}{\omega(n)}+\frac{1}{\Omega(n)}\sum_{i=1}^{r}a_i\log b_i\geq 0. \tag{16}$$

Therefore, we have the inequality $D(n||d)\geq D(n||\gamma(n))$.

5. Conclusions

Present work proposes a new concept the entropy of natural numbers. This concept is a synthesis of the concept of entropy, used for a random variable and the concept of prime number. The significance of the entropy from information point of view is the expected value of the information contained in a message. On the other site the prime factors of a natural number can be considered the generators of this number. Using these interpretations we consider the entropy of a natural number like the measure of order of this number structure. We will remember that a prime number entropy is zero which is the minimum entropy i.e. has the meaning of maximum order. At contrary a natural number with more than one factor, which have the multiplicity of one, have the maximum entropy (whit maximum disorder meaning).The concept of natural numbers entropy is very attractive and we hope that it will lead to benefits in several fields like information theory, numerical theory etc.

References

[1] T. Cover, J. Thomas: *Elements of information theory*, Wiley-Interscience, New Jersey, 2006.

[2] M. Nathanson: *Elementary Methods in Number Theory*, Springer, New York, 2006.

[3] G. Robin: *Estimation de la fonction de Tchebychef* θ *sur le k-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de n*, Acta Arith. 42, 1983, pp. 367-389.

[4] J. Sándor, D. S. Mitrinović, B. Crstici: *Handbook of Number Theory I*, Springer, 1995.

[5] C. Shannon: *A Mathematical Theory of Communication*, The Bell System Technical Journal,Vol. 27, July, October, 1948, pp. 379-423, 623-656.

[6] M. V. Subbarao: *On some arithmetic convolutions in: The Theory of Arithmetic Functions, Lecture Notes in Mathematics*, New York, Springer-Verlag, 1972.