## Article

# An informational test for random finite strings 

<br>1 Department of Computer Science, University of Verona, Italy; vincenzo.bonnici,vincenzo.manca@univr.it<br>* Correspondence: vincenzo.manca@univr.it; Tel.: +39-045-802-7981<br>$\dagger$ Current address: Strada le Grazie 15, 37134 Verona, Italy.<br>$\ddagger$ These authors contributed equally to this work.


#### Abstract

In this paper, by extending some results of informational genomics, we present a new randomness test based on the empirical entropy of strings and some properties of repeatability and unrepeatability of substrings of certain lengths. We give the theoretical motivations of our method and some experimental results of its application to a wide class of strings: decimal representations of real numbers, roulette outcomes, logistic maps, linear congruential generators, quantum measurements, natural language texts, and genomes. It will be evident that the evaluation of randomness resulting from our tests does not distinguish among the different sources of randomness (natural, or pseudo-casual).


Keywords: Algorithmic Information Theory; Incompressibility; Typicality; Randomness Test; Pseudo-random Generators; k-mer Multiplicity; k-Entropy; Informational indexes

## 1. Introduction

The notion of randomness has been studied since the beginning of Probability Theory ("Ars Conjectandi sive Stochastice" is the title of famous Bernoulli's treatise). In time, a lot of connections with scientific concepts were discovered, and random structures have become crucial in many fields, from randomized algorithms to encryption methods. However, very often the lines of investigation about randomness appear no clearly related and integrated. In the following we outline a synthesis of the main topics and problems addressed in the scientific analysis of randomness, for a better understanding of the approach presented in the paper.

### 1.1. Mathematical Definitions of Randomness

The attempts to provide mathematical definitions agreeing with the intuitive meaning of this concept have a very long and complex history $[6,19]$. According to the Algorithmic Information Theory $[5,7,10,13,20,26,29]$ a finite string is random if it is incompressible, that is, the length of any program generating it is always longer than the length of the string (decreased by an additive constant independent from the length of the string). This definition opens a wide spectrum of analyses relating randomness to computation and complexity. Algorithmic Information Theory puts in evidence a strong link relating computation with randomness. This link was also a key point of Martin-Löf's approach to randomness for infinite strings [17]. In particular, a theoretical notion of statistical test was developed by him in terms of computability theory. A sequence is defined random when it passes all recursively enumerable tests by escaping from fulfilling any computable "peculiar" property of strings. In this sense a random string has to be typical, or amorphous, or generic. Already Shannon, in his famous booklet [27] founding Information Theory, used typicality in the proof of his second theorem, by finding that when the string lengths increase the number of non-typical sequences vanishes. Just the lack of any peculiarity of typical sequences is responsible of their incompressibility. However, though, incompressibility and typicality represent significant achievements toward the logical analysis of randomness, they suffer of applicability to real cases. In fact, incompressibility and typicality are not computable properties.

In 1872 Ludwig Boltzmann in the analysis of thermodynamic concepts inaugurated a probabilistic perspective that is the beginning of a new course changing radically the way of considering physical systems. The following theory of quanta developed by Max Plank [28], can be considered in the same line of thought, and quantum theory as it was defined in years 1925-1940 [25] and in the more recent developments [1], confirms the crucial role of probabilistic and entropic concepts in the analysis of physical reality. According to quantum theory, what is essential in physical observations are the probabilities of obtaining some values when physical variables are measured, that is, physical measurement are random variables, or information sources with peculiar probability distributions, because measurements are random processes. This short mention to quantum mechanics want to stress the importance that randomness play in physics and in the whole science, and consequently the relevance of randomness characterizations for the analysis of physical theories. In this paper, we will show that Shannon entropy, related to Boltzmann's H function [15], is a key concept in the development of an new approach to the randomness of finite strings.

### 1.2. True Randomness

"True randomness" concerns with the more intuitive notion of random process as it emerges from nature or from games, such as coin tosses, urn extractions, dices, play cards, and so on. In physics, many phenomena have been discovered, such as Brownian motions of colloidal particles, or measurements in quantum systems, where physical parameters are generated without any apparent rule and with a lack of any pattern. The properties of these phenomena are considered random for their total unpredictability, or for their chaotic behavior.

For example, let us consider a Bernoulli process [8] generated by extractions from a urn containing the same number of white and black balls completely indistinguishable in their physical properties, apart the color, which has no relevance in the extractions from the urn (blind extractions). If we represent a sequence of extractions from the urn (by inserting again the extracted ball in the urn) by means of a $0 / 1$ sequence where 1 stands for white (success) and 0 for black (failure), then we can say that the boolean sequence generated in a Bernoulli process is a true random sequence. In fact the unpredictability of this process is based on the assumption that at any extraction 0 and 1 have the same probability of occur. For analogous arguments, Brownian motions or quantum systems exploit mathematical models that exhibit analogous kinds of statistical homogeneity. The more appropriate term for both such kinds of randomness is "Stochasticity" (from a Greek root with the original meaning of guess). A process where we can only guess events does imply the lack of any underlying rule, but only ignorance or uncertainty about this rule, which we do not know because it is secret or because it is too complex to be managed in a reliable way. This is probably the original intuition about randomness.

In stochastic processes we can define random variables (variable assuming values according to a probability distribution) that follow normal distributions or other distributions related to the normal one. For example, the probability of having $k$ times 1 in a Bernoulli sequence of length $n$ is given by a distribution that for $n$ very large approximates to a normal distribution. Many actual randomness tests are based on agreement with statistical distributions [11].

### 1.3. Pseudo-Randomness and Deterministic Chaos

A line of research, very important from the applicative point of view, is the Theory of pseudo-random generators that is aimed at providing deterministic algorithms generating sequences appearing as true random sequences [11,12], with applications going from bank transaction protocols, to Monte Carlo algorithms, or to criptography. In [11], a detailed and updated historical account of random number generators is given. Surprisingly, the most part of investigations about mathematical characterization of randomness (incompressibility and typicality) are unrelated with the practical methods for producing or testing randomness.

In the second part of 20th century, within the theory of Chaos, another important class of random processes of deterministic nature was discovered, where, despite determinism, an intrinsic kind of
chaos was inherent in their dynamics [18]. Deterministic algorithms were found generating sequences hardly distinguishable from true random processes. Today, many classes of deterministic chaotic algorithms are well-known and applied in many different contexts. Chaotic Dynamics easily transform in random strings. In fact, numbers are generated according to some number representation, therefore there are many ways of extracting strings from these dynamics.

### 1.4. Empirical Randomness

In conclusion, we have mathematical randomness (incompressibility, typicality and more technical specializations of them), true or stochastic randomness, and pseudo-randomness. But how can we judge, in a safe way, when a given string is random according to the considered definitions? In the line of research inaugurated in [9], there are now a great number of randomness tests [11,12,16,21,30]. Almost all of them are of statistical nature and implicitly assume the probabilistic nature of true randomness. Therefore, a string is empirically random when it passes a given set of randomness tests. In this case, randomness can be assessed along a spectrum of possibilities related to the number of passed tests and on the specific measures of randomness assigned by each test. Of course, tests show a good level of credibility only if they judge random what the other criteria qualify accordingly.

In the discussion developed so far we encountered a lot of properties that seem to be related with the intuition of randomness (etymology of "random" is a Latin root for an asymmetric object for hitting in a very irregular and uncontrolled way). Many other notions and subtle differences could be considered. One of them, individuated by a pioneer in the mathematical analysis of random sequences [4,11], is the periodicity/aperiodicity, or more generally, the repeatability/unrepeatability of proper parts. This aspect is the key point of the analysis that we will develop in the next sections. A sequence of $m$ digits is $k$-distributed if any of the $m^{k}$ possible $k$-mers appears with the same frequency in the long run. We say it is $\infty$-distributed if it is $k$-distributed for any $k>1$. Borel [4] called normal to base $m$ a real number whose expansion in base $m$ is $\infty$-distributed. He proved the that almost all real numbers (with respect to the uniform measure) are normal to any base. Normality implies that any possible substring occurs infinitely, but in an aperiodic way, therefore normal numbers are irrational.

Many are the randomness tests that are based on repetitiveness phenomena [11]. However, in this paper we show that certain precise relationships hold between the length of strings and the lengths of $k$-mers that present some specific properties of repeatability and unrepeatability. In this regard, the values $\lg _{m} n$ and $2 \lg _{m} n$ play a critical role, which can be used for evaluating the randomness of strings of length $n$. Moreover, $2 \lg _{m} n$ has a natural interpretation in terms of Shannon's entropy based on the distributions of $k$-mers.

## 2. Informational indexes of strings

Given a string $\alpha$ over an alphabet $A$ of $m$ symbols, then we denote by $D(\alpha)$ the set of all substrings of $\alpha$ and by $D_{k}(\alpha)$ the set of $k$-mers of $\alpha$, that is, the strings of $D(\alpha)$ of length $k$. The function $m u l t_{\alpha}(\beta)$ gives the number of occurrences of substring $\beta$ in $\alpha$. Two important classes of $k$-mers are repeats and hapaxes. The $k$-mer $\beta$ is a repeat of $\alpha$ if $\operatorname{mult}_{\alpha}(\beta)>1$, whereas $\beta$ is a hapax of $\alpha$ if $\operatorname{mult}_{\alpha}(\beta)=1$ (the word hapax comes from a Greek root meaning once). In other words, hapaxes are unrepeatable substrings of $\alpha$.

If $\beta$ is a repeat of $\alpha$, then every substring of $\beta$ is a repeat of $\alpha$ too. Analogously, if $\beta$ is a hapax of $\alpha$, then every string including $\beta$ as substring is a hapax of $\alpha$ too.

In terms of repeats and hapaxes we can define the following indexes that we call informational indexes because they are associated to a string viewed as Information Source in the sense of Shannon's Information Theory. These indexes are very useful in understanding the internal structure of strings. The index

$$
\operatorname{mrl}(\alpha)
$$

(maximum repeat length) is the length of the longest repeats occurring in $\alpha$, while

$$
\operatorname{mhl}(\alpha)
$$

(minimum hapax length)is the length of the shortest hapaxes occurring in $\alpha$. Moreover,

$$
\operatorname{mcl}(\alpha)
$$

(maximum complete length) is the maximum length $k$ such that all possible $k$-mers occur in $\alpha$.
Indexes LG and 2LG, called Logarithmic length and Double logarithmic length are defined by the following equations, where $|\alpha|$ denotes the length os string $\alpha$ ( $m$ is the number of different symbols occurring in $\alpha$ ):

$$
\begin{gathered}
L G(\alpha)=\lg _{m}(|\alpha|) \\
2 L G(\alpha)=2 \lg _{m}(|\alpha|)
\end{gathered}
$$

When $\alpha$ is given by the context, we simply write: $m c l, m h l, m r l, L G, 2 L G$ instead of $\operatorname{mcl}(\alpha), \operatorname{mhl}(\alpha), \operatorname{mrl}(\alpha), L G(\alpha), 2 L G(\alpha)$, respectively. The following propositions follow immediately from the definitions above.

Proposition 1. For $k>m r l$ all $k$-mer of $\alpha$ are hapaxes.

Proposition 2. For $k<m h l$ all $k$-mer of $\alpha$ are repeats.

Proposition 3. For any string $\alpha, m h l \geq m c l$.
Proposition 4. For any string $\alpha$ of length $n$ : $D_{k}(\alpha) \leq n-k+1$ and if $D_{k}(\alpha)=n-k+1$, then all the elements of $D_{k}(\alpha)$ are hapaxes of $\alpha$.

Proposition 5. In any string the following inequality holds:

$$
m c l \leq\lceil L G\rceil
$$

By using mult we can define a probability distributions over $D_{k}(\alpha)$, by setting $p(\beta)=$ mult $_{\alpha}(\beta) /(|\alpha|-k+1)$. The Empirical $k$-Entropy of the string $\alpha$ is given by Shannon's Entropy with respect to the distribution $p$ of $k$-mers occurring in $\alpha$ (we use the logarithm in base $m$ for uniformity with the following discussion):

$$
E_{k}(\alpha)=-\sum_{w \in D_{k}(\alpha)} p(w) \lg _{m} p(w) .
$$

It is well-known [27] that Entropy reaches its maximum for uniform probability distributions. Therefore, when all the $k$-mers of a string $\alpha$ of length $n$ occur with the uniform probability $1 /(n-k+1)$. This means that the following proposition holds.

Proposition 6. If all $k$-mers of $\alpha$ are hapaxes, then $E_{k}(\alpha)$ reaches its maximum value in the set of probability distributions over $D_{k}(\alpha)$.

## 3. A "positive" notion of random string

It is not easy to tell when a string is a random string, but it is easy to decide when a given string is not a true random string. A "negative" approach to string randomness could be based on a number of conditions $C_{1}, C_{2}, \ldots$ each of which implies non-randomness. In this way, when a string
does not satisfies any of such conditions, we have a good guarantee of its randomness. In a sense, mathematical characterizations of randomness are "negative" definitions based on infinite sets of conditions. Therefore, even if these sets are recursively enumerable, randomness cannot be effectively stated.

Now, we formulate a principle that is a sort of Borel's normality principle for finite strings. It expresses a general aspect of any reasonable definition of randomness. In informal terms, at this principle says that any substring has the same probability of occurring in a random string, and for substring under a given length, the knowledge of any prefix of a random string does not give no information about their occurrence in the remaining part of the string. In this sense, a random string is a global structure where no partial knowledge is informative about the whole structure.

Principle 1 (Random Log Normality Principle (RLNP)). In any finite random string $\alpha$, of length $n$ over $m$ symbols, for any value of $k \leq n$, all possible $k$-mers have the same a priori probability $1 / m^{k}$ of occurring at each position $i$, for $1 \leq i \leq n-k+1$. Moreover, let us define the a posteriori probability that a $k$-mer occurs at position $i$ as the conditional probability of occurring when the prefix of $\alpha[1, i-1]$ is given. Then, for any $k<2\lceil L G\rceil$, at each position $i$ of $\alpha$, for $1 \leq i \leq n-k+1$, the a posteriori probability of any $k$-mer occurrence has to remain the same as its a priori probability.

The reader may wonder about the choice of the $2\lceil L G\rceil$ bound that appears in RLNP principle stated above. It is motivated by Proposition 7 that is proved by using the first part of RLNP principle.

In the following, a string is considered to be random if it satisfies the RLNP principle. Let us denote by $R N D_{m, n}$ the set of random strings of length $n$ over $m$ symbols, and by $R N D$ the union of $R N D_{m, n}$ for $n, m \in \mathbb{N}$ :

$$
R N D=\bigcup_{n, m \in \mathbb{N}} R N D_{m, n}
$$

For individual strings, in general, RLNP can hold only admitting some degree of deviance from the theoretical pure case. This means that randomness of an individual string cannot be assessed as a $0 / 1$ property, but rather, in terms of some measure expressing the closeness to the ideal cases (for example the percentage of positions where RLNP fails).

According to this perspective, RLNP, may not exactly hold in the whole set $R N D_{m, n}$. Nevertheless, the subset of $R N D_{m, n}$ on which RLNP fails has to approximate to the empty set, or better to a set of zero measure, as $n$ increases. In other words, random strings are "ideal" strings by means of which the degree of similarity to them can be considered as a "degree of membership" of individual strings to RND. This lack of precision is the price to pay for having a "positive" characterization of string randomness.

The following proposition states an inferior length bound for the hapaxes of a random string.
Proposition 7. For any $\alpha \in R N D_{m, n}$ if:

$$
k \geq\lceil 2 L G\rceil
$$

then all $k$-mers of $\alpha$ are hapaxes of $\alpha$.
Proof. Let us consider a length $k$ such that:

$$
m^{k} \geq n-k+1
$$

According to RLNP, the probability that a $k$-mer occurs in $\alpha \in R N D_{m, n}$ is given by the following ratio (the number of available positions of $k$-mers is $n-k+1$ ):

$$
\begin{equation*}
\operatorname{Prob}\left(\alpha \in D_{k}(\alpha)\right)=\frac{(n-k+1)}{m^{k}} \tag{1}
\end{equation*}
$$

but, if all $k$-mers are hapaxes in $\alpha$, then their probability of occurring in $\alpha$ is also given by:

$$
\begin{equation*}
\operatorname{Prob}\left(\alpha \in D_{k}(\alpha)\right)=\frac{1}{(n-k+1)} \tag{2}
\end{equation*}
$$

then, if we equate the right members of the two equations above (1) and (2), we obtain an equation that has to be satisfied by any length $k$ ensuring that all $k$-mers occurring in $\alpha$ are hapaxes in $\alpha$ :

$$
\begin{equation*}
(n-k+1)^{2}=m^{k} \tag{3}
\end{equation*}
$$

that implies:

$$
\begin{equation*}
2 \lg _{m}(n-k+1)=k \tag{4}
\end{equation*}
$$

In order to evaluate the values of $k$, we solve the equation above by replacing $k$ in the left member of Equation (4) by the whole left member of Equation (4):

$$
\begin{equation*}
2 \lg _{m}\left(n-2 \lg _{m}(n-k+1)+1\right)=k \tag{5}
\end{equation*}
$$

now, the equation (5) implies that:

$$
\begin{equation*}
2 \lg _{m}\left(n-2 \lg _{m}(n)\right) \leq k \leq 2 \lg _{m}(n) \tag{6}
\end{equation*}
$$

but the difference between the two bounds of $k$ is given by:

$$
2 \lg _{m}(n)-2 \lg _{m}\left(n-2 \lg _{m}(n)\right)=2 \lg _{m} \frac{n}{n-2 \lg _{m}(n)}=2 \lg _{m}\left(1+\frac{2 \lg _{m} n}{n-2 \lg _{m} n}\right)
$$

where the right member approximates to zero as $n$ increases. In conclusion:

$$
k \approx 2 \lg _{m}(n)
$$

This means that for:

$$
k \geq\left\lceil 2 \lg _{m}(n)\right\rceil=\lceil 2 L G\rceil
$$

all $k$-mers of $\alpha$ are hapaxes, that is, $\lceil 2 L G\rceil$ is a lower bound for all unrepeatable substrings of $\alpha \in R N D_{m, n}$.

The following proposition follows as a direct consequence of previous proposition and Proposition 1.

Proposition 8. If $\alpha \in R N D$ then:

$$
m r l+1=\lceil 2 L G\rceil .
$$

In conclusion we have shown that in random strings $2 L G$ is strictly related to mrl index.

According to the proposition above the index $2 L G$ has a clear entropic interpretation: $i l$ is the value of $k$ such that the empirical entropy $E_{k}$ of a random string reaches its maximum value.

We have seen that in random strings all substrings longer than $\lceil 2 L G\rceil$ are unrepeatable, but what about the minimum length of unrepeatable substrings? The following proposition answers to this question, by stating a upper bound for the length of repeats in random strings

Proposition 9. If $\alpha \in R N D$ then:

$$
m h l \leq\lceil L G\rceil
$$

Proof. Let us consider $k=\lceil L G\rceil$. If some of such $k$-mers is a hapax, the proposition is proved. Otherwise, if no $k$-mer is a hapax of $\alpha$, then all $k$-mers of $\alpha$ are repeats. But, this fact is against the Random Log Normality Principle (RLNP). Namely, in all the positions $i$ of $\alpha$ such that in $\alpha[1, i]$ a $k$-mer $\beta$ occurs once (these positions necessarily exist), the a posteriori probability that $\beta$ has of occurring in a position $i+1$ of $\alpha$ after is $1 /(n-k-i)$, surely greater than $1 / m^{k}$ (where $\left.n=|\alpha|\right)$. Hence, in positions after $i$ the a posteriori probability would be different from the a priori probability. In conclusion, if $\alpha \in R N D$ some hapaxes of length $\lceil L G\rceil$ have to occur in $\alpha$, thus necessarily $m h l \leq\lceil L G\rceil$.

Our analysis shows that in random strings there are two bounds given by $\lceil L G\rceil$ and $2\lceil L G\rceil$. Under the first one we have only repeatable sub-strings, while over the second one we have only unrepeatable sub-strings. The agreement with these conditions and the degrees of deviance from them give an indication about the randomness degree of a given string.


Figure 1. The logarithmic bounds of Randomness.
It is easy to provide examples of strings where these conditions are not satisfied, but what is interesting to remark is that the conditions hold with a very strict approximation for strings that pass usual randomness statistical tests, moreover for "long strings", for example genomes, the bounds hold, but in a very sloppy way because usually $m r l+1$ is considerably greater than $\lceil 2 L G\rceil$ and $m h l-1$ is considerably smaller that $\lceil L G\rceil$.

In our findings reported in Section 5, the best randomness was found for strings of $\pi$ decimal digits, for quantum measurements and for strings obtained by pseudo-casual generators[24]. In next sections we discuss our experimental data about our randomness parameters.

## 4. Log Bounds Randomness Test

The Log-Bounds-Test (LBT), based on the analysis developed in the previous sections, essentially checks, for a given string, the logarithmic bounds for its prefixes, and in the average (with the standard deviation). We apply LBT to a wide class of strings, in order to verify if it correctly guesses the randomness of strings traditionally judged random, and at the same time, if it does not give such an evidence in the cases where it is not appropriate. The results confirm a discrimination capability with a complete accordance with our expectations.

For our analyses we have taken into account different types of strings that are commonly considered as random strings, available in public archives.

A first category of random strings is extracted from a real numbers such as $\pi$ and Euler's constant $e$. In this case, the number is converted into a string over the alphabet of decimal digits, and a given number of digits of the number $e$ are extracted. Digits were download at https:/ /www.angio.net/pi/ digits/ pi1000000.txt and https:/ / apod.nasa.gov/htmltest/ gifcity/e.2mil.

Quantum physics generated data based on the non-determinism of photon arrival times, provide up to $150 \mathrm{Mbits} / \mathrm{s}$ in the form of series of bytes, available at http:/ / qrng.physik.hu-berlin.de/.

Another category of random data is given by mathematical functions that provide chaotic dynamics, such as the logistic map with parameter in $[3.8,4]$.

Linear congruential generators of the form $x_{n+1}=c x_{n}+b$ generate pseudo-random numbers $[11,12]$ that we converted into strings of suitable alphabets of different sizes by applying discretization mechanisms.

Another category is given by random series related to roulette spins, cards, dices, and Bernoulli urns. In particular, we took into account 3 million consecutive roulette spins produced in the Spielbank Wiesbaden casino, at the website https:/ /www.roulette30.com/2014/11/free-spins-download.html As it is already recognized by several authors, randomness of roulette data is not true randomness, and this was also confirmed by our findings.

For comparisons we used non-random data given by the complete works of Shakespeare available at http:/ /norvig.com/ngrams/shakespeare.txt. These texts were transformed in order to extract from them only letters by discarding other symbols.

We used another comparison text given by the complete genome of the Sorangium cellulosum bacterium, downloaded from the RefSeq/NCBI database at https:/ /www.ncbi.nlm.nih.gov / nuccore/ NC_010162.1 (with a length of around 13 millions nucleotides).

## 5. Analysis of the experimental results

When the informational indexes $m h l$ and $m r l+1$ will result to coincide with $L G \pm 1$ and $2 L G \pm 1$ respectively, we consider this coincidence as a positive symptom of randomness and we will mark this fact by writing $\checkmark$ on the right of the compared values (or $X$ in the opposite case). The more these coincidences are found for prefixes of a string, the more the string passes our test (a more precise evaluation could consider not only the number of coincidence, but also how much the values differ, when they do not coincide). As tables in the next section show, Our findings agree, in a very significant way, with the usual randomness/nonrandomness expectations. Tables are given for different categories of strings. Informational indexes were computed by a specific platform for long string analysis [3]. In Table 1, from 100.000 up to 30 Millions of decimal expansions of $\pi$ are considered. The agreement with our theory is almost complete, whence very high level of randomness is confirmed, with only a very slight deviance.

Other tables are relative to decimal expansions of other real numbers: Table 2 for Euler's constant, Table 3 for $\sqrt{2}$ and Table 4 for Champernowne's constant, a real transcendent number obtained by a non-periodic infinite sequence of decimal digits (the concatenated decimal representations of all natural numbers in their increasing order).It is interesting to observe that Euler's constant and $\sqrt{2}$ have behaviors similar to $\pi$, whereas Champernowne's constant has values indicating an inferior level of randomness.

Table 5 concerns with strings coming from the pseudo-casual Java generator (a linear congruential generator). The randomness of these data, with respect to our indexes, is very good.

Table 6 is relative to strings generated via the logistic map. In these cases randomness is not so clearly apparent, due to a sort of tendency to having patterns of periodical nature, which agree with already recognized behaviors due to the limits of computer number representations [22].

Table 7 provides our indexes for quantum data [24], by showing a perfect agreement with a random profile.

Finally, Table 9 and Table 10 are relative to a DNA bacterial genome, and to texts of natural language (Shakespeare's works) respectively. In these cases, as expected, our indexes of randomness reveal low levels of randomness.

## 6. Conclusions

In this paper we presented an approach to randomness that extends previous results on informational genomics (information theory applied to the analyses of genomes [2,14]), where the analysis of random genomes was used for defining genome evolutionary complexity. A general analysis of randomness has emerged that suggests a line of investigation where a theoretical approach is coupled with a practical and experimental viewpoint, as required by the application of randomness to particular situations of interest. Randomness has an intrinsic paradoxical, and at same time vague, nature. In fact, mathematical rigorous definitions of randomness are intrinsically uncomputable, and algorithmically testable properties are not exhaustive.

We introduced Random Log Normality Principle, which resembles Borel's Normality [11], but it is formulated, for finite strings, in terms of a priori and a posteriori probabilities. This principle allows us to define two logarithmic bounds that state precise links between the length of strings and the lengths to which specific phenomena of substring repetitiveness must or cannot hold.

A possible continuation of our investigation could be addressed to extend similar principles and tests for finite structures, such as tree or graphs. In fact, in many applications it would be very useful having reliable and simple tests for finite mathematical structures commonly used in data representations.

## 7. Tables

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 100,000 | 4 | 5 | $\checkmark$ | 10 | 10 | $\checkmark$ |
| $1,000,000$ | 5 | 6 | $\checkmark$ | 13 | 12 | $\checkmark$ |
| $2,000,000$ | 6 | 7 | $\checkmark$ | 13 | 14 | $\checkmark$ |
| $5,000,000$ | 6 | 7 | $\checkmark$ | 13 | 14 | $\checkmark$ |
| $10,000,000$ | 6 | 7 | $\checkmark$ | 15 | 14 | $\checkmark$ |
| $20,000,000$ | 7 | 8 | $\checkmark$ | 15 | 16 | $\checkmark$ |
| $50,000,000$ | 7 | 8 | $\checkmark$ | 16 | 16 | $\checkmark$ |

Table 1. Decimal digits of $\pi$.

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 100,000 | 4 | 5 | $\checkmark$ | 10 | 10 | $\checkmark$ |
| 200,000 | 5 | 6 | $\checkmark$ | 12 | 12 | $\checkmark$ |
| 500,000 | 5 | 6 | $\checkmark$ | 12 | 12 | $\checkmark$ |
| $1,000,000$ | 5 | 6 | $\checkmark$ | 13 | 12 | $\checkmark$ |
| $1,200,000$ | 5 | 7 | $\mathbf{x}$ | 13 | 14 | $\checkmark$ |
| $1,500,000$ | 6 | 7 | $\checkmark$ | 13 | 14 | $\checkmark$ |
| $2,000,000$ | 6 | 7 | $\checkmark$ | 13 | 14 | $\checkmark$ |

Table 2. Decimal digits of Euler's constant $e$.

| $n$ | MHL | $\lceil L G\rceil$ | Check | MRL + 1 | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 10,000 | 4 | 4 | $\checkmark$ | 8 | 8 | $\checkmark$ |
| 20,000 | 4 | 5 | $\checkmark$ | 8 | 10 | $\boldsymbol{x}$ |
| 50,000 | 4 | 5 | $\checkmark$ | 10 | 10 | $\checkmark$ |
| 100,000 | 4 | 5 | $\checkmark$ | 11 | 10 | $\checkmark$ |
| 200,000 | 5 | 6 | $\checkmark$ | 11 | 12 | $\checkmark$ |
| 500,000 | 5 | 6 | $\checkmark$ | 11 | 12 | $\checkmark$ |
| $1,000,000$ | 5 | 6 | $\checkmark$ | 12 | 12 | $\checkmark$ |

Table 3. Decimal digits of $\sqrt{2}$.

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 10 | 1 | 2 | $\checkmark$ | 2 | 3 | $\checkmark$ |
| 100 | 2 | 2 | $\checkmark$ | 3 | 4 | $\checkmark$ |
| 1,000 | 3 | 3 | $\checkmark$ | 6 | 6 | $\checkmark$ |
| 10,000 | 4 | 4 | $\checkmark$ | 9 | 8 | $\checkmark$ |
| 100,000 | 5 | 5 | $\checkmark$ | 12 | 10 | $x$ |
| $1,000,000$ | 5 | 6 | $\checkmark$ | 15 | 12 | $\checkmark$ |
| $10,000,000$ | 6 | 7 | $\checkmark$ | 18 | 14 | $x$ |

Table 4. Decimal digits of Champernowne's constant.

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 100 | 2 | 2 | $\checkmark$ | 4 | 4 | $\checkmark$ |
| 1,000 | 3 | 3 | $\checkmark$ | 6 | 6 | $\checkmark$ |
| 10,000 | 4 | 4 | $\checkmark$ | 8 | 8 | $\checkmark$ |
| 100,000 | 4 | 5 | $\checkmark$ | 10 | 10 | $\checkmark$ |
| $1,000,000$ | 5 | 6 | $\checkmark$ | 12 | 12 | $\checkmark$ |
| $10,000,000$ | 6 | 7 | $\checkmark$ | 14 | 14 | $\checkmark$ |

Table 5. Pseudo-random decimal numbers generated by Java linear congruential generator.

Author Contributions: Conceptualization, V.M.; methodology, V.B and V.M.; software, V.B.; validation, V.B. and V.M.; formal analysis, V.M.; investigation, V.B. and V.M.; resources, V.B.; data curation, V.B.; writing-original draft preparation, V.M.; writing-review and editing, V.M.; visualization, V.B.; supervision, V.M.; project administration, V.M.; funding acquisitioand V.M.

Funding: This research received no external funding

Acknowledgments: The authors thank people of the Center for BioMedical Computing of the University of Verona, for the stimulating discussions concerning the topic of the paper

Conflicts of Interest: Authors declare no conflict of interest

## References

1. Bell, J., S. Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy. Cambridge University Press (2004)
2. Bonnici, V., Manca, V. Informational Laws of genome structures. Scientific Reports, 6, 28840, (2016)
3. Bonnici, V. , Manca, V. Infogenomics tools: A computational suite for informational analysis of genomes. J. Bioinformatics \& Proteomics Review 1, 8-14 (2015)
4. Borel, E. Les probabilities denomerable et leurs applications arithmetiques.Rend. Circ. Mat. Palermo, 27, 247-271 (1909)
5. Chaitin, G. J. On the length of programs for computing finite binary sequences: statistical considerations. J. Assoc. Comput. Mach., 16, 145-159 (1969)
6. Church, A. On the concept of a random sequence. Bulletin of the Am. Math. Soc. 46, 130-135 (1940)
7. Downey, R. G. Hirschfeldt, D. R. Algorithmic Randomness and Complexity. Springer (2010)
8. Feller, W. Introduction to Probability Theory and its Applications. John Wiley \& Sons Inc. (1968)
9. Knuth, D. E. The art of computer programming, Vol. 2, Semi-numerical Algorithms, Addison-Wesley (1981)

| $n$ | MHL | [LG] | Check | MRL + 1 | 「2LG〕 | Check |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| Alphabet size 10 |  |  |  |  |  |  |
| 10 | 1 | 2 | $\checkmark$ | 2 | 4 | $x$ |
| 50 | 1 | 2 | $\checkmark$ | 7 | 4 | $x$ |
| 100 | 1 | 2 | $\checkmark$ | 10 | 4 | $x$ |
| 200 | 2 | 3 | $\checkmark$ | 11 | 6 | $x$ |
| 500 | 2 | 3 | $\checkmark$ | 14 | 6 | $x$ |
| 1,000 | 2 | 3 | $\checkmark$ | 17 | 6 | $x$ |
| 10,000 | 2 | 4 | $x$ | 21 | 8 | $x$ |
| 100,000 | 2 | 5 | $x$ | 32 | 10 | $x$ |
| 1,000,000 | 2 | 6 | $x$ | 35 | 12 | $x$ |
| 5,000,000 | 2 | 7 | $x$ | 39 | 14 | $x$ |
| 10,000,000 | 2 | 7 | $x$ | 42 | 14 | $x$ |
| 52,000,000 | 2 | 8 | $x$ | 61 | 16 | $x$ |
| Alphabet size 1,000 |  |  |  |  |  |  |
| 10 | 1 | 2 | $\checkmark$ | 2 | 4 | $x$ |
| 50 | 1 | 2 | $\checkmark$ | 3 | 4 | $\checkmark$ |
| 100 | 1 | 2 | $\checkmark$ | 3 | 4 | $\checkmark$ |
| 200 | 1 | 2 | $\checkmark$ | 5 | 4 | $\checkmark$ |
| 500 | 1 | 2 | $\checkmark$ | 8 | 4 | $x$ |
| 1,000 | 1 | 2 | $\checkmark$ | 8 | 4 | $x$ |
| 10,000 | 1 | 2 | $\checkmark$ | 18 | 4 | $x$ |
| 100,000 | 2 | 2 | $\checkmark$ | 25 | 4 | $x$ |
| 1,000,000 | 2 | 2 | $\checkmark$ | 28 | 4 | $x$ |
| 5,000,000 | 2 | 3 | $\checkmark$ | 34 | 6 | $x$ |
| 10,000,000 | 2 | 3 | $\checkmark$ | 38 | 6 | $x$ |
| 52,000,000 | 2 | 3 | $\checkmark$ | 52 | 6 | $x$ |

Table 6. Strings generated by logistic maps with seed 0.1 and parameter $r=4$. Generated numbers are normalized in the interval $(0,1)$ and thus discretized into 10 and 1000 digits.

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | MRL + 1 | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 100,000 | 2 | 3 | $\checkmark$ | 5 | 6 | $\checkmark$ |
| 500,000 | 2 | 3 | $\checkmark$ | 6 | 6 | $\checkmark$ |
| $1,000,000$ | 3 | 3 | $\checkmark$ | 6 | 6 | $\checkmark$ |
| $5,000,000$ | 3 | 3 | $\checkmark$ | 6 | 6 | $\checkmark$ |
| $10,000,000$ | 3 | 3 | $\checkmark$ | 7 | 6 | $\checkmark$ |
| $50,000,000$ | 3 | 4 | $\checkmark$ | 7 | 8 | $\checkmark$ |

Table 7. Raw quantum data (alphabet size 256).

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 100,000 | 3 | 4 | $\boldsymbol{\checkmark}$ | 7 | 8 | $\boldsymbol{\checkmark}$ |
| 200,000 | 3 | 4 | $\boldsymbol{\checkmark}$ | 31 | 8 | $\boldsymbol{x}$ |
| 500,000 | 3 | 4 | $\boldsymbol{\checkmark}$ | 31 | 8 | $\boldsymbol{x}$ |
| $1,000,000$ | 4 | 4 | $\boldsymbol{\checkmark}$ | 315 | 8 | $\boldsymbol{x}$ |
| $1,500,000$ | 4 | 4 | $\boldsymbol{\checkmark}$ | 315 | 8 | $\boldsymbol{x}$ |
| $2,000,000$ | 4 | 5 | $\boldsymbol{\checkmark}$ | 315 | 10 | $\boldsymbol{x}$ |
| $2,500,000$ | 4 | 5 | $\boldsymbol{\checkmark}$ | 315 | 10 | $\boldsymbol{x}$ |
| $3,000,000$ | 4 | 5 | $\boldsymbol{\checkmark}$ | 315 | 10 | $\boldsymbol{x}$ |

Table 8. Roulette spins (alphabet size 37).
10. Kolmogorov, A. N. Three approaches to the quantitative definition of information. Problems of Information Transmission, 1,1-7 (1965)
11. L'Ecuyer, P. History of Uniform Random Number Generation. Proceedings of the 2017 Winter Simulation Conference, 202-230 (2017)
12. L'Ecuyer, P. Random Number Generation with Multiple Streams for Sequential and Parallel Computers. Proceedings of the 2015 Winter Simulation Conference, IEEE Press, 31-44 (2015)
13. Li, M., Vitany, P. An Introduction to Kolmogorov Complexity and its Applications, Springer-Verlag (1997)

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 100 | 2 | 4 | $\boldsymbol{x}$ | 8 | 7 | $\boldsymbol{l}$ |
| 1,000 | 3 | 5 | $\boldsymbol{x}$ | 14 | 10 | $\boldsymbol{x}$ |
| 10,000 | 4 | 7 | $\boldsymbol{x}$ | 17 | 14 | $\boldsymbol{x}$ |
| 100,000 | 5 | 9 | $\boldsymbol{x}$ | 116 | 17 | $\boldsymbol{x}$ |
| $1,000,000$ | 6 | 10 | $\boldsymbol{x}$ | 381 | 20 | $\boldsymbol{x}$ |
| $10,000,000$ | 7 | 12 | $\boldsymbol{x}$ | 2,721 | 24 | $\boldsymbol{x}$ |
| $13,033,770$ | 7 | 12 | $\boldsymbol{x}$ | 2,721 | 24 | $\boldsymbol{x}$ |

Table 9. Sorangium cellulosum's genome (alphabet size 4).

| $n$ | $M H L$ | $\lceil L G\rceil$ | Check | $M R L+1$ | $\lceil 2 L G\rceil$ | Check |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 10,000 | 1 | 3 | $\boldsymbol{x}$ | 25 | 6 | $\boldsymbol{x}$ |
| 100,000 | 2 | 4 | $\boldsymbol{x}$ | 42 | 8 | $\boldsymbol{x}$ |
| 200,000 | 2 | 4 | $\boldsymbol{x}$ | 117 | 8 | $\boldsymbol{x}$ |
| 500,000 | 2 | 5 | $\boldsymbol{x}$ | 287 | 10 | $\boldsymbol{x}$ |
| $1,000,000$ | 2 | 5 | $\boldsymbol{x}$ | 287 | 10 | $\boldsymbol{x}$ |
| $1,500,000$ | 2 | 5 | $\boldsymbol{x}$ | 287 | 10 | $\boldsymbol{x}$ |
| $2,000,000$ | 2 | 5 | $\boldsymbol{x}$ | 287 | 10 | $\boldsymbol{x}$ |
| $2,500,000$ | 2 | 5 | $\boldsymbol{x}$ | 287 | 10 | $\boldsymbol{x}$ |
| $3,000,000$ | 2 | 5 | $\boldsymbol{x}$ | 286 | 10 | $\boldsymbol{x}$ |
| $3,301,740$ | 2 | 5 | $\boldsymbol{x}$ | 286 | 10 | $\boldsymbol{x}$ |

Table 10. Shakespeare's collection (alphabet size 26).
14. Manca, V. The Principles of Informational Genomics. Theoretical Computer Science, 701, 190-202 (2017)
15. Manca, V. An informational proof of H-Theorem. Open Access Library Journal, Vol. 4, e3396 (2017)
16. Marsaglia, G. DIEHARD: a battery of tests of randomness. http:/ / stat.fsu. edu/ geo/diehard.html (1996)
17. Martin-Löf, P. The definition of random sequences,Information and Control, 9, 602-619 (1966)
18. May, R. M. Simple mathematical models with very complicated dynamics. Nature 261, 459-67 (1976).
19. Mises von R. Grundlagen der Wahrscheinlichkeitsrechnung. Mathematische Zeitschrift, 5, 52-99 (1919)
20. Nies, A., Computability and Randomness, Oxford University Press (2009)
21. NIST: National Institute of Standards and Technologies. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Gaithersburg, MD 20899-8930 (2010)
22. Persohn, K. J. Povinelli, R. J. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. Chaos, Solitons \& Fractals, 45, 238-245 (2012)
23. Planck, M. Planck's Original Papers in Quantum Physics. Annotated by H. Kangro, translated by Haar, ter D.; Brush, S. G. Taylor \& Francis: London, 1972.
24. Pu L., Xiaohang, Y. Xianglian, L., Yunkay, W., Yongge, W. Brownian motion properties of optoelectronic random bit generators based on laser chaos. Optics Express, 24, 14, 15822 (2016)
25. Purrington, R. D. The Heroic Age. The Creation of Quantum Mechanics 1925-1940. Oxford Univ. Press (2018)
26. Schnorr, C.P., A unified approach to the definition of random sequences. Math. Systems Theory, 5, 246 (1971)
27. Shannon, C. E. A mathematical theory of communication. Bell Sys Tech J, 27, 623-656 (1948)
28. Sharp, K. Matschinsky, F. Translation of Ludwig Boltzmann's Paper "On the Relationship between the Second Fundamental Theorem of the Mechanical Theory of Heat and Probability Calculations Regarding the Conditions for Thermal Equilibrium". Entropy 17, 1971-2009 (2015)
29. Solomonoff, R. J. A formal theory of inductive inference, I,Information and Control, 7, 1-22 (1964)
30. Soto, J. Statistical testing of random number generators, http:// csrc.nist.gov/rng/ (1999)

