An Information Theoretic Analysis of Random Number Generator based on Cellular Automaton

Amirahmad Nayyeri
Division of Computer Science, Faculty of Science
Salman Farsi University of Kazerun, Kazerun, Iran

Gholamhossein Dastghaibyfard
Computer Engineering and IT Department
Shiraz University, Shiraz, Iran

***Abstract*—Realization of Randomness had always been a controversial concept with great importance both from theoretical and practical Perspectives. This realization has been revolutionized in the light of recent studies especially in the realms of Chaos Theory, Algorithmic Information Theory and Emergent behavior in complex systems. We briefly discuss different definitions of Randomness and also different methods for generating it. The connection between all these approaches and the notion of Normality as the necessary condition of being unpredictable would be discussed. Then a complex-system-based Random Number Generator would be introduced. We will analyze its paradoxical features (Conservative Nature and reversibility in spite of having considerable variation) by using information theoretic measures in connection with other measures. The evolution of this Random Generator is equivalent to the evolution of its probabilistic description in terms of probability distribution over blocks of different lengths. By getting the aid of simulations we will show the ability of this system to preserve normality during the process of coarse graining.**

Keywords*—Random number generators; entropy; correlation information; elementary cellular automata; reversibility

I. Introduction to Randomness

Realization of randomness has great importance both from theoretical and practical perspective. The successful application of randomness for guiding search processes in spaces which scales exponentially to the input size shows the theoretical importance of having access to a proper source of randomness [1]. One can show generally that the existence of proof for theorem T with specific length n can be reduced to combinatorial problem of finding a tour of length $\leq B$ that reaches all N cities while $N = poly(n)$ [2].

Although the concept of Randomness has entered literarily by the theory of probability, this theory cannot define the randomness associated with individual objects whether finite or infinite. Probability theory is a theory about sets of objects not individual objects. Therefore it cannot distinguish between two sequences of length n generated on binary alphabet $\{0,1\}$ in which one of them consists of just ones and the other corresponds to the tossing of a fair coin. It turns out that realization of randomness is very challenging and this concept resists theoretical investigation. Historically scientists have tried to define it in a specific domain. Fortunately one can observe the source of problem as a main thread in all of these domain specific approaches.

Von Mises [3] was the first person who tried to define randomness mathematically based on an intuitive aspect of unpredictability. He described randomness as an inability to predict the elements of an infinite binary sequence over $\{0,1\}$ with probability better than½ while the elements in the string are chosen randomly. Then he tried to improve his definition by replacing the random selection of elements with an acceptable selection rule. Evidently this change did not increase the mathematical clarity of his definition. Subsequently Wald [4, 5] introduced the notion of countability of selection function in order to make this definition more clear. Finally Mises's definition was refined in the light of computability of selection functions by Church [6]. Therefore acceptable selection rules were replaced by computable functions and as such the theoretical realization of randomness integrated with the notion of computability.

This type of evolved definition is known as Mises-Wald-Church definition [7]. Although Mises-Wald-Church definition of randomness was criticized by other thinkers like Ville [8], it kept its theoretical effect on subsequent works in this area.

The relation between randomness and computability has been deepened in the light of modern interpretation of defining and detecting randomness relatively to the amount of computational sources which have been used [9]. The notion of randomness is measured in its modern formulation for finite objects by Kolmogorov complexity [10], [11] which is the result of Solmonof, Kolmogorov and Chaitins theory [12] and for infinite objects by the Mrtin-Lof measure of randomness [13], [14].

These new definition of randomness are deeply connected to the theory of computation. The Kolmogorov complexity of a string x is defined as the size of the shortest program that produces it. Obviously random strings must have higher Kolmogorov complexity due to their incompressibility. Therefore the Kolmogorov complexity of random string x, denoted by $C(x)$ would be approximately equals to length of string x. Formally $C(x) \approx |x|$ and random strings cannot be compressed [10]. Introducing finite random objects as incompressible objects connects the notion of randomness to the philosophical interpretation of theory which was presented for the first time by Leibniz [15].

Philosophically, theory is recognized as a compression form of statements which can describe a set of large experimental data in the shortest way. Otherwise the theory with the same size of data set, which it explains would be

useless. In section V of Discourse de Metaphysique, Leibniz explains the comprehensibility of the world as the result of God's creation, in which the greatest possible diversity of phenomena are controlled by the smallest set of ideas. Today this fact can be rephrased in the language of algorithmic randomness. It means in spite of this apparent diversity in the world the set of rules which are responsible for all these phenomena is small. Therefore we can follow a scientific method to discover the theory which explains a set of wide natural phenomena. Based on this perspective the set of random data would be theory-less. Chaitin's Ω number is recognized as an incompressible sequence of zeros and ones. This number is the probability of halting for program P generated by a successive independent tosses of a fair coin. Mathematically Ω is defined by (1)[16].

$$\Omega = \sum_{P\ halts} 2^{-(size\ in\ bits\ of\ P)} \quad (1)$$

Ω is an example of algorithmically irreducible or random string. The bits of Ω cannot be compressed. In other words, its bits are true for a reason not simpler than itself. This breaking of Leibniz's famous principle of sufficient reason is one of the most controversial aspect of randomness in philosophy. It must be mentioned that Chaitin's result about halting probability is in fact another type of Godel's famous Incompleteness theorem [16]. Today we know that proving the randomness of a finite string$x$, is an example of incompleteness phenomena.

The computability of selection function in the Mises-Wald-Church definition of randomness for finite objects can be observed in terms of effective measure for continuous objects in Martin-Lof definition [14]. A real number x is considered random, if x is not contained in any event of effective measure zero [14].

The unpredictability as an intuitive notion of randomness plays a great role in other approaches for defining randomness. Ville [8] tried to define randomness by gambling approach. In his definition, it is impossible to win an infinite amount of money by betting on the bits of a random binary sequence. The amalgamation of the theory of randomness and the theory of computation has provided the opportunity of using theoretical apparatuses developed in the theory of computation to analyze the randomness in a deeper way.

Today we know the set of strings which are random in the sense of Kolmogorov complexity is not even computably enumerable and because of that, the statement of the form: x is a random string, is not provable [16].

In addition to the previous results, randomness in its modern formulation is considered relatively. In the light of the theory of computability, we interpret randomness in contrast to the amount of computational sources, used to detect it [17].

Although randomness has been always seen as a sign of complexity especially in the lack of causal model, in recent years, it has been realized that randomness is responsible for emergence of many complex phenomena by providing the opportunity of having interactions between many agents in systems. There is a tendency to disentangle randomness from complexity. For a recent work on this please refer to [18]. It is believed that complexity in its own true form is the result of directed interactions between elements of system.

Randomness and its mysterious aspects have played a great role especially in fertilizing the multidisciplinary studies at the crossroad of mathematics, physics and computer science. Using random resources for solving hard problems in Randomized Algorithms has been very advantageous [19] both in substantial reduction of time complexity and also in deepening of our understanding of the nature of hard problems.

After the seminal work of Russel impagliazzo and Avi Wigderson about the tradeoff between hardness and randomness [20], today we know the importance of having randomized algorithm for solving hard problems as a theoretical key for designing deterministic algorithms.

There is no doubt that nature uses randomness extensively in the evolution. In recent years, Gregory Chaitin has started working on Metabiology [21]. He is studying the random evolution of artificial software in order to realize Busy Beaver function as a fitness function. The soul of his technique has been based on applying randomness as it has been applied in evolution in terms of mutation.

This paper has been organized into 6 sections. After this introduction about randomness, Random generators and their categorization and applications will be reviewed in Section 2. In Section 3, Cellular Automaton is formally defined and its application as Random generator will be discussed. Primary information Theoretic measures are explained in Section 4. These measures are used to analyze our inhomogeneous ECA60 as a Random Generator in Section 5 and finally in Section 6, concluding remarks will be presented.

II. Random Generator

The difficulties of giving a complete definition of randomness were discussed briefly in the previous section. Randomness in its modern formulation is considered as a relative concept. Therefore Random Generators must satisfy criteria which guarantee their efficiency for the specific application.

The success of simulations which are based on Monte Carlo method is highly dependent on the quality of their random generators [22]-[25]. The security of information transfer on internet and the cryptography need random generators [26]. Randomness and Random generators are used extensively in solving hard problems in the framework of stochastic optimization and naturally inspired algorithm in order to bypass the problem of getting stuck in local extremes [27]-[29].

Random generators play a key role in many techniques of program validation [30] and Machine learning [31]. The rational behavior in strategic zero sum games needs to use randomness and Random Generators to mislead the opponent [32]. In recent years, Random Generators are used for Analyzing and simulation of interactions in complex social, economical and political systems at different scales [33]-[35].

Historically three approaches have been followed for generating randomness although there are many controversial

issues about the possibility of producing intrinsic randomness. True Random Number Generators (TRNG) use physical phenomena with inherent stochastic mechanism for generating random numbers [36]. There are many phenomena which can be used for TRNGs, for example unstable nuclear decay processes [37], cosmic background radiation [38], quantum based systems [39]-[41] and more exotic examples like superconducting nanowires and Josephson junctions near superconducting critical current [42].

The randomness of physical source can be amplified in some cases [43] provided that fundamental theoretic limits are preserved [44], although Santha and Vazirani proved that randomness amplification is impossible using classical resource [45].

The next family of generators is called Random Number Generators (RNG). In these generators randomness is transformed from a priori distribution in source to the desired posterior distribution [46], therefore these generators have an access to sources of randomness.

RNGs are categorized to three main groups: Von Neumann RNG [47] in which an identically independent priori distribution is transformed to the unbiased random numbers. Knuth and Yao RNG [48], in which an identically independent prior distribution is transformed to any desired distribution in output and finally Roche and Hoshi RNG [49], [50] which transform an arbitrary random distribution in source to an arbitrary distribution in output.

The third family of generators for generating randomness is called Pseudo-Random Number Generators (PRNG) in which arithmetical methods are used in order to produce randomness. Although John Von Neumann once said [47] "Anyone who considers arithmetical methods for producing random digits is, of course, in the state of sin", Chaos theory shows how randomness can emerge from deterministic systems, while we have a hypersensitive dynamic to the initial states [51], [52].

Therefore, in the light of Chaos Theory, there is a deep dichotomy between order and randomness. This fact provides the opportunity of applying deterministic algorithms for generating randomness. Hence, PRNGs try to generate randomness without having access to any source of randomness [53]-[56].

III. Cellular Automata and Random Generators

Cellular Automata were created by John Von Neumann, in his attempt to create a self-replicating machine [57]. He tried to show that, these machines are universal constructors and can generate even themselves. Cellular Automata have found a better place in theoretical studies when Stephen Wolfram published his book, called A New Kind of Science [58]. In this book he tried to present an extensive analysis of these systems and their effectiveness to realize a wide range of natural phenomena which are common to exhibit a particular type of behavior known as Emergent behavior.

Elementary Cellular Automata (ECA) is defined on alphabet set $A = \{0,1\}$ as 1-dimensional cellular array of size$N$. The state of each cell i at time t is denoted by $s_i^t \in A$. The global state or lattice configuration of Cellular Automaton at time t is represented byS^t, where $S^t = (s_0^t, s_1^t, \dots, s_{N-1}^t) \in A^N$($N$ is the size of lattice) [59].

All cells in the lattice are updated according to local update function f which generally has $2r + 1$ arguments, where r is the radius of local function ($r = 1$ in Elementary Cellular Automata). Formally s_i^{t+1} is defined by local function$f$.

$$s_i^{t+1} = f(s_{i-r}^t, \dots, s_i^t, \dots, s_{i+r}^t) \quad (2)$$

Applying f to all cells simultaneously, leads to the formation of next global state and maps S^t to S^{t+1} under the action of global function$F: A^N \to A^N$. It has been conjectured that applying very simple local function f at micro scale can give rise to a very complicated behavior in macro scale [58]. This highly interesting behavior is called Emergence and has inspired an extensive type of studies [60].

Cellular Automata were used for the first time as Pseudo-Random Generator by Wolframe [61], [62]. Actually he used the unpredictable emergent behavior of the global function in Cellular Automata resulted from simultaneous application of local function on different cells, as a main mechanism for generating randomness.

Afterwards, people tried to improve the quality of CA's random generator by using a combination of controllable cells [63], increasing the dimensionality of Cellular Automata [64]-[66], changing the neighborhood of cells [67], using Cellular Automata with additive rules [68], applying the evolutionary principles for designing Cellular Automata [69] and focusing on the parallelism associated with the evolution of global state in Cellular Automata for generating randomness [70].

Stephen wolfram in his well-known book "The New Kind of Science" categorized elementary Cellular Automata into four families [58]. The states of cells in elementary Cellular Automata are selected from simple binary alphabet set $\{0,1\}$ and the radius of their local function r is equal to one. It is believed that in spite their simplicity, Elementary Cellular Automata (ECA) show all types of behaviors which can be observed in Cellular Automata in higher dimensions and with more complex local functions. Since the number of possible Elementary Cellular Automata is limited to$2^{2^3} = 256$, these systems have been examined from different perspectives [71], [72].

As an evidence for the power of ECA and the mysterious aspects of emergent behavior at macro scale in complex systems, like Cellular Automata, coordinated by simple interactions between cells at micro scales, please refer to [73] in which Emergent behavior has been used in combination with other complex system's properties for generating pseudo-randomness. It turns out that this strategy can generate randomness which does not have any dependency on the initial values of the system.

In this paper, a modified type of an Elementary Cellular Automaton (ECA60) would be used as random generator and its evolution from random initial state would be analyzed information theoretically. In the next section, primary Information measures will be introduced briefly.

IV. INFORMATION THEORETIC MEASURES

Our goal in this paper is to analyze the capability of a modified type of Elementary Cellular Automaton 60, the number of which is assigned according to Wolfram's rule, as a random generator. The system is initialized by a random binary sequence on alphabet set {0, 1}. During the evolution of Elementary Cellular Automaton, this random initial sequence of size N is transformed to other sequence of size$N$, while it preserves the initial randomness and simultaneously shows dynamical reversibility. It avoids building correlations in the evolution while all of the initial information at each time step is transformed to the next global state and because of this conservative behavior and dissipation-less dynamic the initial state of the system would be observed again. The periodicity of this conservative behavior is$O(N)$. In order to analyze this behavior, we use information theoretic measures.

Elementary Cellular Automaton with rule number 60 has been used as a random generator in which the central cell in local configurations 101,100, 011 and 010 is transformed to 1 and the central cell in the remaining four configurations 000,001,110 and 111 is transformed to 0, except for the first cell s_0^t, which is transferred without change to the next generation. As we will observe in the following section, this direct transfer of first cell is responsible for the reversibility of system. The evolution of our random generator from random initial state is shown in Fig. 1.

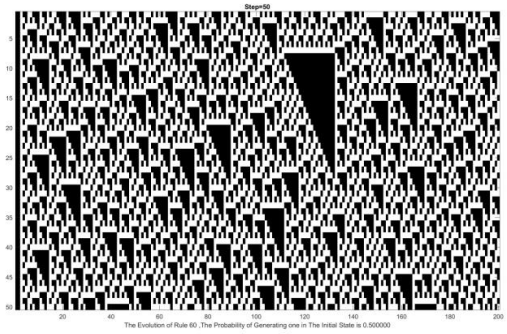

Fig. 1. The evolution of ECA60 from random initial configuration of size 200 during 50 generations.

The system is initialized by random global state, consisting of zeroes and ones (here our alphabet set is $A = \{0,1\}$). Randomness implies that, starting from the beginning of system, one cannot predicate the next symbol in the sequence by observing its previous symbols. Statistically it means:

$$\lim_{i\to\infty,k\to\infty} P(x_i|x_{i-1}, \dots\dots, x_{i-k+1}) = \frac{1}{|A|} \quad (3)$$

Here, randomness has been interpreted as a uniform distribution on the characters of alphabet which is led to the maximum possible entropy rate.

The entropy function which measures the average of uncertainty can be defined over substring of global state of length$n$, provided that conditions in (4) and (5) are satisfied [74].

$$P(\delta_n) \geq 0, where\ \delta_n \in A^n \quad (4)$$

$$\sum_{\delta_n \in A^n} P(\delta_n) = 1 \quad (5)$$

Furthermore, it is assumed that sequences are generated by the stationary stochastic process. The Ergodicity of generator is preserved due to the nature of local function in Elementary Cellular Automata [74].

These substrings are in fact the microstates of the system upon which macro state S^t is built. Technically, the famous method of describing macro state in terms of probabilistic mass function over its constituent microstates in statistical physics has been applied. Therefore, the probabilistic description of the system's global state called $P_n = \{p_i\}_{i=1}^n$, defines the Probability Mass Function (PMF) over system's microstates.

Having in mind such probabilistic description of the system, the entropy of system is defined by (6) provided $n \to \infty$ [75].

$$S_n = S[P_n] = \sum_{\delta_n} P(\delta_n) \log_2 \frac{1}{P(\delta_n)} \quad (6)$$

Actually S_n quantifies the disorder of n-length subsequences of the global string S^t at generation$t$. Usually S_n increases as n(the size of substrings or microstates) grows, but the action of local function$f$ makes certain correlations, which mitigates the growth of disorder proportional to the length of microstates. The maximum entropy associated with each character which is selected from alphabet set$A$, is $\log_2 |A|$ and consequently in the case of pure randomness, the maximum entropy of $n \log_2 |A|$ for sequence δ_n of length n over alphabet set$A$ is expected to be observed.

The correlation can be detected as the result of $S_n - S_{n-1}$ becomes less than $\log_2 |A|$ (the maximum amount of entropy per symbol when the characters are chosen from set$A$). But this reduction $(S_n - S_{n-1})$ may be the result of correlations which have been built at much lower lengths. In order to detect the correlation specifically at length n, one can compare the consecutive gaps in entropy, computed on blocks of lengths $n-2, n-1$ and$n$. Consequently, correlation at length$n$ in (7) is calculated.

$$K_n = (S_{n-1} - S_{n-2}) - (S_n - S_{n-1}) = \Delta S_{n-1} - \Delta S_n \quad (7)$$

All correlations which have been formed at lengths less than n are considered in ΔS_{n-1}, hence if there is correlation at length n, ΔS_n must be less than ΔS_{n-1} and their difference is purely related to K_n(Correlation at length n). Although there are different approaches for calculating correlations, one can observe the simple phenomenon which produces it at specific distance. Formally the emergence of correlation at length n requires (8) to be met.

$$P(x_n|x_{n-1}, \dots\dots, x_1) > P(x_n|x_{n-1}, \dots\dots, x_2) \quad (8)$$

The maximum amount of entropy per symbol is decomposed to the entropy rate of the system and all the

correlations which have formed at different lengths. Mathematically it means [74]:

$$S_{max} = \log_2 |A| = \Delta S_\infty + \sum_n K_n \quad (9)$$

V. Analyzing the Random Generator

The modified version of ECA60 has been used as a Random Generator which transforms an initial random sequence into another random sequence in the next generation. This transformation is done against our normal expectation to observe the increment of regularity in the sequence, due to the applying of deterministic local function. Fortunately the system is able to preserve the initial randomness during its evolution in spite of having a considerable hamming distance between consecutive global states of the system. It means that, this conservation of randomness would not decrease the activity of system.

As Lindgren [74] showed in Elementary Cellular Automata, due to the deterministic nature of local function, we expect the global entropy to be decreased during the evolution of system. Mathematically it means $\Delta_t S(t) = S(t+1) - S(t) \leq 0$. this fact can be realized intuitively, since applying local function $f: \{0,1\}^3 \rightarrow \{0,1\}$ in Elementary Cellular Automata is usually accompanied with the omission of variations in the system's global state and would force system to converge to the very small subset of all possible global states. Obviously moving toward regularity and reduction of variations would lead to decrementing of the initial randomness. This behavior is not suitable for our purpose. On the other side it can be shown that $\Delta_t S(t)$ is zero for systems with conservative nature [74].

It is not hard to realize that $\Delta_t S(t)$ would be zero for almost reversible systems, i.e. entropy is constant during the evolution. A Cellular Automaton with rule R and range r is called almost reversible if R can be decomposed in the following way [74]:

$$R(x_1, x_2, \dots, x_{2r+1}) = f(x_1, x_2, \dots, x_{2r}) + x_{2r+1} mod 2 \quad (10)$$

Or

$$R(x_1, x_2, \dots, x_{2r+1}) = x_1 + f(x_2, x_3, \dots, x_{2r+1}) mod 2 \quad (11)$$

It means R is one to one if one can support it by giving it the information about its first or last argument. It is easy to show that our random generator is an almost reversible rule since its local function can be written as:

$$f(x_{i-1}^t, x_i^t, x_{i+1}^t) = x_i^t XOR x_{i-1}^t = (x_{i-1}^t + x_i^t) mod 2 = x_i^{t+1} \quad (12)$$

Therefore f is reversible if we have an access to the value of x_{i-1}^t or x_i^t. In order to recover the global state at time t from the global state at time $t+1$, we can use the following equation inductively for $= 1,2, \dots, n-1$, when n is the size of system, if we have an access to the first bit of global state at time $t(x_0^t)$.

$$x_i^t = (x_{i-1}^t + x_i^{t+1}) mod 2 \quad (13)$$

Please remember that our Random Number Generator is an inhomogeneous type of ECA60 in which the state of first cell in the system is transformed to the next generation without change. In fact, having access to this single bit from the previous generation makes us able to recover all the bits of previous state by applying (13), iteratively. Generally in Almost Reversible Rule with range r, one can recover the previous state by having access to the $2r$-bits of the previous generation [74].

As a matter of fact we are taking the advantage of emergence to produce next random sequence from the current one. This emergence here manifests itself as complex global function induced by simultaneous applying of local function f to all cells in the system. Generally there is no mathematical method to find the relation between global function F and local function f in such systems.

Conservation of information in this Random Generator which is leaded to the conservation of initial randomness due to the (9) is related to the global reversibility of Cellular Automata.

Studies by Hedlund [76] and Richardson [77] have shown that for Cellular Automaton A, A is injective if it is invertible (Reversible). Therefore reversibility in CA is equivalent to the injectivity of its global function. Furthermore A is injective if it is surjective and there is a close relation between injectivity and surjectivity of the Cellular Automaton A.

Injectivity and Surjectivity for global functions of CA's were studied by Moore [78] and Myhill [79] for the first time in the way of analyzing Garden of Eden (a global state without predecessor). Studies about the reversibility of dynamical systems have attracted many attentions on the part of scientists. We know that physical world at micro scale is governed by reversible rules. Surprisingly what can be observed at macro scale is irreversible. It is believed that this irreversibility at macro scale motivated by reversible rules at micro scale can be interpreted as a sign of Emergence in the system [60].

In addition to that, studies about Reversibility has found an extra importance after the seminal work of Landauer [80]. He found a relation between consuming energy and irreversibility in dynamical systems. In other words, he showed that dissipation of heat in the system which is the main source of consuming energy has its root in erasing information during the process in the system. Erasing information happens in irreversible systems, in which one cannot recover the information of previous state by having the information of current state. Although it is not hard to imagine that every irreversible process would be accompanied by erasing information, Landauer [80] predicted the minimum amount of energy dissipation associated with erasing one bit. Recently his prediction has been verified experimentally [81]. It has been shown by Bennett [82] that it is possible to do any computation reversibly. It means we have a reversible analogue for Universal Turing Machine. Then people started to analyze the advantages of reversibility in computing system [83]. It is exciting to know that in principle, reversible computation can be done with zero energy consumption. Many fundamental

limits to the computation process were realized better in the light of these studies [84]. Due to the importance of reversibility, many algorithms have been developed in order to detect it in the variety of dynamical systems [85], [86]. It has been shown that deciding the reversibility or its equivalent property in systems with dimension higher than one is impossible [87], [88].

In spite of conservative nature of this Random Generator, the initial random configuration is transformed into another random configuration with considerable hamming distance with previous global state. Furthermore the normality of random binary sequence is kept during the evolution of system. Let's look at the definition of normality and normal sequence.

Normality demands the balanced form of appearance for all patterns which means every block of digits of the same length occurs with the same frequency when all digits in the expansion are considered. Normality can be interpreted in the light of information theoretic measures. Although there are other similar concepts which are related to notion of normality, one has to know that random sequences must be normal in order to satisfy their expected unpredictability.

It is expected that unpredictability demonstrates itself as our inability to forecast the dominant frequency of observing specific pattern. Normality can be described with the aid of other measures like block complexity, block entropy, etc.

Definition [89]: the block complexity of a sequence with values in a finite alphabet is the function $k \to P(k)$, where $P(k)$ is the number of different blocks of length k that occur in the sequence.

Clearly for a sequence over alphabet set A with length k, block complexity satisfies the (14).

$$1 \le P(k) \le |A|^k \tag{14}$$

For normal sequences, maximum block complexity is expected. Obviously low block complexity would not be seen in random sequence and can be responsible for generating periodic behavior. It is interesting to realize how block complexity as a local measure for sub-sequences can be used to predict the global behavior of the sequence. Morse and Hedlund proved the following theorem about this relation.

Theorem [90]: if the complexity of a sequence satisfies $\exists k \ge 1\ P(k) \le k$, then the sequence is ultimately periodic.

The block complexity can easily be related to block entropy. In section 4, the block entropy for the global state of a Cellular Automaton was defined when the process responsible for generating it is ergodic. When the block complexity for blocks of length k over alphabet set A is equal to $|A|^k$, it can be concluded that every possible pattern of length k over this alphabet set has been generated; therefore, maximum entropy would be expected. There is a simple relation between block complexity and block entropy. Considering their definition we can simply reach to (15).

$$H(B_n) = S_n = \frac{logP(B_n)}{\log|A|} \tag{15}$$

Here A is a binary set therefore (14) can be simplified into $H(B_n) = logP(B_n)$. As we discussed before, the entropy rate would be calculated when the length of block tends to infinity and all correlations are considered. Thus we have:

$$h = \lim_{n\to\infty} \frac{H(B_n)}{n} = \lim_{n\to\infty} \frac{\log P(B_n)}{nlog(|A|)} = \lim_{n\to\infty} \frac{logP(B_n)}{n} \tag{16}$$

When the length of block tends to infinity, the correlations among symbols at different lengths exhibit themselves as a restriction of freedom for choosing among the possible $|A|$ characters of alphabet. Therefore in the case of having correlations, the block complexity is not increased proportionally to the length of the block and the normality is broken. In other words for a sequence δ_n of length n with correlations among its characters we have $P(\delta_n) < |A|^n$.

Since the correlation at specific length n is accompanied by the reduction of growth in block complexity at length n in contrast to its growth at length $n-1$ it can be detected when the entropy rate is decreased at some specific length. In Fig. 2, the entropy rate over blocks of size 10 for a system of size 10^6, over 100 generation has been shown.

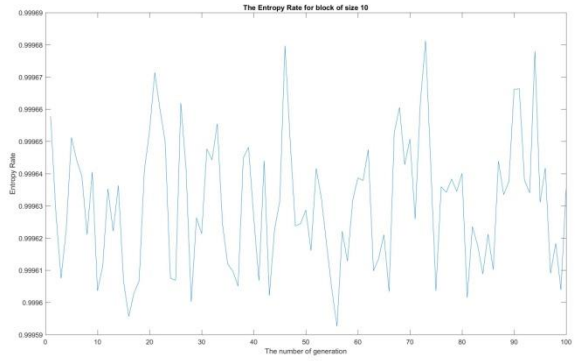

Fig. 2. The entropy rate for system of size 10^6 over blocks of size 10 for 100 consecutive generations.

The entropy rate shows fluctuations in the scale of 10^ (-5) over generations. Furthermore the lower value of entropy rate for blocks of size 10 is bigger than 0.99 which approves of the random nature of sequences generated by this random generator since the maximum entropy rate for our system is $\log|A| = log2 = 1$.

In this Random Generator, the block complexity is much more than the lower threshold predicated by Morse & Hedlund [90], [91] and it is around $2^{nh_\mu} \approx 2^{9.9} \gg 10$. Surprisingly here in spite of keeping considerable local variations and nearly maximum block complexity, the global state of system shows periodicity due to its conservative nature of system and the trajectory of global state starting from initial configuration meets the initial state again. Fortunately in its entire route from initial state, the normality at different lengths is preserved because the entropy rate does not depict considerable difference calculated on blocks of different sizes. In Fig. 3, the entropy rate for system of size 10^6 over 200 generation has been displayed when the entropy rate is calculated over blocks of different lengths ranging from 5 to 10.

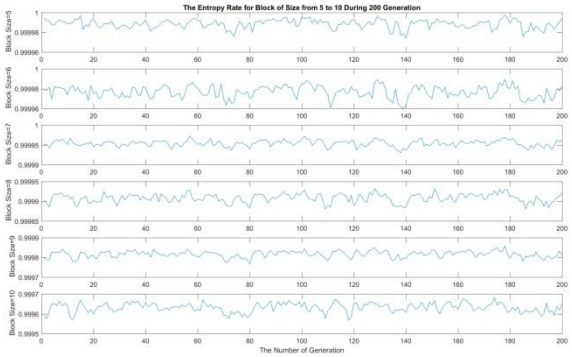

Fig. 3. The entropy rate for system of size 10^6 over blocks of different lengths ranging from 5 to 10 during 200 generations.

Fortunately the conservation of information does not impose restriction on the micro-dynamic of system and consecutive global states have considerable hamming distance. Please see the Fig. 4.

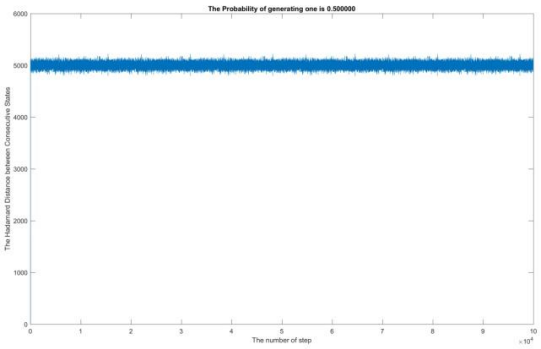

Fig. 4. the hamming distance between consecutive generations for system of size 10000 during 10^5 generations.

VI. Discussion and Conclusion

The work of this Random Generator can be analyzed from different perspectives such as the Conservation of initial information during the evolution leads to reversible dynamic, the intrinsic parallelism (as the result of simultaneous updates of cells in the system), the efficient use of initial randomness and the ability of generating acceptable number of sequences which are equivalent to the initial configuration considering their randomness or their entropy rate. In other words this Random Generator is able to show varied behavior while it keeps its initial information during its evolution.

Taking into account (9) as the Hamiltonian of this Random Generator, the maximum amount of entropy rate of the system can be decomposed into the entropy of the system or its random parts plus its regular parts which are the result of summing all of its correlations at different lengths. Actually in this system, the random part of the current global state is mapped into the random part of the next global state. The fluctuations in the entropy rate calculated over blocks of different lengths are negligible and can be the result of encoding randomness from one length into another. Furthermore due to its avoidance of building correlations or empowering them, the Normality of generated sequences is preserved during the evolution at all scales.

Preservation of Normality at all scales and the conservative nature of this Random Generator, in spite of having considerable micro-activity turn this system into remarkable Random Generator. In addition, this Random Generator gets the benefits of intrinsic parallelism and proves to be technically easy to implement due to its simple logical local function.

References

[1] H. H. Holger, S. Thomas, Stochastic Local Search: Foundations and Applications, Elsevier, 2005.

[2] J. Garey, M. R. Garey, D. S. Johnson, Computers and Interactability, Freeman Press, 1979.

[3] M. R. Von, "Grundlagen der Wahrscheinlich Keit Srechung," Mathematische Zeit schrift, 5, pp. 52-99, 1919.

[4] A. Wald, "Sur La Notion de Collectif Dans La Calcul Des Probabilities," Comptes Rendus Des Seances De l'Scademie Des Sciences, 202, pp. 180-183, 1936.

[5] A. Wald, "Die Wiederspruchsfreiheit Des Kollektiv Begriffes Der Wahrscheinlich keitscrechnung," Ergebnisse Eines Mathematischen Kolloquiums, 8, pp. 38-72, 1937.

[6] A. Church, "On the Concept of Random Sequence," Bulletin of the American Mathematical Society, 46, pp. 130-135, 1940.

[7] S. A. Terwijn, "The Mathematical Foundations of Randomness," In the Challenge of Chance, K. Landsman and E. Van Wolde(Editors), pp. 49-66, Springer, 2016.

[8] J. Ville, "Etude Critique De La Notion De Collectif, Monographies Des Probabilities," Calcul Des Probabilites et Ses Applications, Gauthier-Villars, 1939.

[9] A. Nies, Computability and Randomness, Oxford University press, 2009.

[10] M. Li, P. Vitanyi, An Introduction to Kolmogorov Complexity and Its Applications (3rd Edition), Springer, 2008.

[11] G. Chaitin, "On the Length of Programs for Computing Finite Binary Sequences," Journal of ACM, 13(145), 1966.

[12] H. Zenil, Randomness through Computation Some Answers More Question, World Scientific, 2011.

[13] R. G. Downey, D. R. Hirschfeldt, A. Nies, S. A. Terwijn, "Calibrating Randomness," Bulletin of Symbolic Logic, vol. 12(3), pp. 411-491, 2006.

[14] P. Martin-Lof, "the Definition of Random Sequences, Information and Control," vol. 9, pp. 602-619, 1966.

[15] G. W. Leibniz, Discourse de Metaphysique, Svivide Monadologie, Gallimard, 1995.

[16] G. Chaitin, Thinking about Godel and Turing: Essays on Complexity, World scientific, 2007.

[17] S. Arora, B. Boaz, Computational Complexity: A Modern Approach, Cambridge University Press, 2009.

[18] L. Zuchowski, "Disentangling Complexity From Randomness and Chaos," Entropy, 14, pp. 177-212, 2012.

[19] J. Hromkovic, Design and Analysis of Randomized Algorithms: Introduction to Design Paradigms, Springer, 2005.

[20] R Impagliazzo, A. Wigderson, "P=BPP if E Requires Exponential Circuits: Derandomizing the Xor Lemma," in Proceeding of the 29th Annual ACM Symposium on the Theory of Computing, pp. 220-9, 1997.

[21] G. Chaitin, Proving Darwin: Making Biology Mathematical, Pantheon Book, 2012.

[22] J. Gentle, Random Number Generation and Monte Carlo Methods, 2nd Edittion, Springer, 2003.

[23] PL. Ecuyer, "Random Numbers for Simulation," Communication of ACM, vol. 33, pp. 85-97, 1990.

[24] R. Y. Rubinstein, D. P. Kroese, Simulation and the Monte Carlo Method, John Wiley & Sons, 2011.

[25] J. E. Gentle, Random Number Generation and Monte Carlo Methods, Springer, 2013.

[26] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, 2005.

[27] J. Carmelo, A. Bastos-Filho, D. Jaulio, D. Andrade, R. Marcelo, S. Pita et al. "Impact of the Quality of Random Numbers Generations on the Performance of Particle Swarm Optimization," In IEEE International Conference on Systems, Man and Cybernetics, pp. 4988-93, 2009.

[28] A. Reese, "Random Number Generators in Genetic Algorithms for Unconstrained and Constrained Optimization," Nonlinear Analysis Theory Methods & Application, vol. 71, pp. 679-92, 2009.

[29] A. Brabazon, M. O'Neill, S. McGarraphy, Natural Computing Algorithms, Springer, 2015.

[30] R. G. Sargent, "Verification and Validation of Simulation Models," In Proceeding of the 37th Conference on Winter Simulation, pp. 130-143, 2005.

[31] E. Alpaydin, Introduction to Machine Learning, MIT Press, 2014.

[32] J. H. Conway, On Numbers and Games, Volume 6, IMA, 1976.

[33] J. M. Epstein, Generative Social Science: Studies in Agent-Based Computational Medeling, Princeton University Press, 2006.

[34] J. M. Epstein, Agent-Zero: Toward Neurocognitive Foundation for Generative Social Science, Princeton University Press, 2013.

[35] O. Dowlen, The Political Potential of Sortition: A Study of the Random Selection of Citizens for Public Office, Volume 4, Andrews UK Limited, 2015.

[36] C. D. Motchenbacher, F. C. Fitchen, Low-Noise Electronic Design, John Wiley & Sons, 1973.

[37] G. F. Knoll, Radiation Detection and Measurement, John Wiley & Sons, 2010.

[38] N. Yoshida, R. K. Sheth, A. Diaferio, "Non-Gaussian Cosmic Microwave Background Temperature Fluctuation from Peculiar Velocities of Clusters," Monthly Royal Astronomy Society, vol. 328(2), pp. 669-677, 2001.

[39] T. Jennewein, U, Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, "A Fast and Compact Quantum Random Number Generator," Rev. Sci. Instr., vol. 71(4), pp. 1675-1680, 2000.

[40] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, H. Zbinden, "Optical Quantum Random Number Generator," Journal of Modern Optics, vol. 47(4), pp. 595-598, 2000.

[41] A. Acin, L. Masanes, "Certified Randomness in Quantum Physics," Nature, vol. 540, pp. 213-219, 2016.

[42] M. Foltyn, M. Zgirski, "Gambling with Super-Conducting Fluctuations," Physical Review Application, vol. 4(2), 024002, 2015.

[43] R. Colbeck, R. Runner, "Free Randomness Can be Amplified," Nature Physics, vol. 8, pp. 450-454, 2012.

[44] S. Pironi et al., "Random Number Certified by Bell's Theorem," Nature, vol. 464, pp. 1021-1024, 2010.

[45] M. Santa, U. V. Vazirani, "Generating Quasi-Random Sequences from Semi-Random Sources," Journal of Computing System Science, vol. 33, pp. 75-87, 1986.

[46] L. Devroye, "Sample-Based Non-Uniform Random Variable Generation," In Proceeding of the 18th Conference on Winter Simulation, ACM, pp. 260-265, 1986.

[47] J. V. Neumann, "Various Techniques Used in Connection with Random Digits," National Bureau of Standards Applied Math Series, pp. 36-38, 1963.

[48] D. E. Knuth, A. C. Yao, the Complexity of Non-Uniform Random Number Generation, Academic Press, 1976.

[49] J. R. Roche, "Efficient Generation of Random Variables from Biased Coins," Proceeding of IEEE international Symposium in Information Theory, pp. 169, 1991.

[50] M. Hoshi, "Interval algorithm for Random Number Generation," IEEE Transaction on Information Theory, vol. 43(2), pp. 599-611, 1997.

[51] A. Kanso, "Search-Based Chaotic Pseudo-Random Bit Generator," Internatinal Journal of Bifurcation and Chaos, vol. 19, no. 12, pp. 4227-4235, 2009.

[52] R. Lozi, "Emerging of Randomness from Chaos," International Journal of Bifurcation and Chaos, vol. 22, no. 2, pp. 1250021, 2012.

[53] B. A. Wichmann, I. D. Hill, "Algorithm AS 183: An Efficient and Portable Pseudo-Random Number Generator," Journal of Royal Statistic Society Series C, vol. 31(2), pp. 188-190, 1982.

[54] L. Blum, M. Blum, M. Shub, "A Simple Unpredictable Pseudo-Random Number Genertor," SIAM Journal of Computing, vol. 15(2), pp. 364-383, 1986.

[55] M. Mascagni, S. A. Cuccaro, D. V. Pryor, M. L. Robinson, "A Fast High Quality and Reproducible Parallel Lagged Fibonacci Pseudo-Random Number Generator," Journal of Computational Physics, vol. 119(2), pp. 211-219, 1995.

[56] J. K. Salmon, M. A. Moraes, R. O. Dror, D. E. Shaw, "Parallel Random Numbers: As Easy As 1 2 3," International Conference for High Performance Computing Networking Storage and Analysis, IEEE, pp.1-12, 2011.

[57] J. V. Neumann, Theory of Self-Replicating Automata, Edited and Completed by A. W. Burks, University of Illinois press, 1966.

[58] S. Wolfram, A New Kind of Science, Wolfram Media, 2002.

[59] N. Boccara, Modeling Complex Systems, Second Edition, Springer, 2010.

[60] B. Falkerburg, M. Morrison, Why More is Different: Philosophical Issues in Condensed Matter Physics and Complex Systems, Springer, 2015.

[61] S. wolfram, "Cryptography with Cellular Automata," In Proceeding of the CRYPTO 85, Advances in Cryptography, vol. 218, pp. 429-32, 1985.

[62] S. Wolfram, Theory and Applications of Cellular Automata, River Edge, NJ:World Scientific, pp. 1983-6, 1986.

[63] S. U. Guan, S. Zhang, "a Family of Controllable Cellular Automata for Pseudo-Random Generation," International Journal of Modern Physics C, vol. 13(8), pp. 1047-73, 2002.

[64] M. S. Tomassini, M. Sipper, M. Perrenoud, "On the Generation of High Quality Random Numbers by Two-Dimensional Cellular Automata," IEEE Transactions on Computer, vol. 49, pp. 1146-51, 2000.

[65] B. Kang, D. Lee, C. Hong, "Pseudorandom Number Generation Using Cellular Automata," In Novel Algorithms and Techniques in Telecommunication Automata and Industrial Electronics, pp. 401-4, 2008.

[66] S. Shin, G. Park, K. Yoo, "A Virtual Three-Dimensional Cellular Automata Pseudorandom Number Generator Based on More Neighborhood Method," In 4th International Conference on Intelligent Computing, ICIC 2008, pp. 174-81, 2008.

[67] S. Shin, K. Yoo, "Analysis of 2-state 3-neighborhood Cellular Automata Rules for Cryptographic Pseudorandom Number Generation," In International Conference on Computational Science and Engineering, CSE 2009, pp. 399-404, 2009.

[68] P. Chaudhuri, D. Chowdhurry, S. Nardi, S. Chattopadhyay, Additive Cellular Automata: Theory and Application, vol. 1, IEEE Computer Society Press, 1997.

[69] S. Guan, S. Zhang, "An Evolutionary Approach to the Design of Controllable Cellular Automata Structure for Random Generation," IEEE Transaction on Evolutionary Computing, vol. 7, pp. 3-6, 2003.

[70] P. Hortensius, R. Mcleod, H. Card, "Parallel Random Number Generation for VLSI system Using Cellular Automata," IEEE Transaction on Computing, vol. 38, pp. 1466-73, 1989.

[71] R. Dogaru, I. Dogaru, H. Kim, "Synchronization in Elementary Cellular Automata," In Proceedings of the 10th International Workshop on Multimedia Signal processing and Transmission, CMSPT 2008, pp. 35-40, Jeonju, Korea, July 21-22, 2008.

[72] R. Dogaru, I. Dogaru, H. Kim, "Binary Chaos Synchronization in Elementary Cellular Automata," International Journal of Bifurication & Chaos, vol. 19, pp. 2871, 2009.

[73] S. M. Hossseini, H. Karimi, M. Vafaei Jahan, "Generating Pseudorandom Numbers by Combining two Systems with Complex Behaviors," Journal of Information Security and Applications, vol. 9, pp. 149-162, 2014.

[74] K. Lindgren, Information Theory for Complex Systems, Chalmers University Press, 2014.

[75] J. T. Cover, J. A. Thomas, Elements of Information Theory, Wiley, 2006.

[76] G. Hedlund, "Endomorphisms and Automorphisms of the Shift Dynamical System," Mathematical System Theory, vol. 3, pp. 320-375, 1969.

[77] D. Richardson, "Tesselations with Local Transformations," Journal of Computing System Society, vol. 6, pp. 373-388, 1972.

[78] E. Moore, "Machine Models of Self-Reproduction," Proceeding of Syposia in Applied Mathematics, American Mathematical Society, vol. 14, pp. 17-33, 1962.

[79] J. Myhill, "The Converse of Moore's Garden of Eden Theorem," Proceeding of American Mathematical Society, vol. 14, pp. 658-686, 1963.

[80] R. Landauer, "Irreversibility and Heat Generation in the Computing Process," IBM Journal of Research & Development, vol. 5, pp. 183-191, 1961.

[81] A. Berut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, E. Lutz, "Experimental Verification of Landauer's Principle Linking Information and Thermodynamics," Nature, vol. 483, pp. 187, 2012.

[82] C. H. Bennett, "Logical Reversibility of Computation," IBM Journal of Research & Development, vol. 17, pp. 525-532, 1973.

[83] C. H. Bennett, "The Thermodynamics of Computation," International Journal of Theoretical Physics, vol. 21, pp. 905-940, 1982.

[84] C. H. Bennett, "The Fundamental Physical Limits of Computation," Scientific American, vol. 253, pp. 38-46, 1985.

[85] K. Sutner, "De Bruijn Graphs and Linear Cellular Automata," Complex Systems, vol. 5(1), pp. 19-30, 1991.

[86] T. Head, "Linear CA: Injectivity for Ambiguity," Complex Systems, vol. 3(4), pp. 343-348, 1989.

[87] J. Kari, "Reversibility of 2D Cellular Automata is Undecidable," Physica D, vol. 45, pp. 397-385, 1990.

[88] J. Kari, "Reversibility and Surjectivity Problems of Cellular Automata," Journal of Computing System Science, vol. 48, pp. 149-182, 1994.

[89] J. P. Allouche, Algebraic and Analytic Randomness, In Noise Oscillation and Algebraic Randomness Edited by M. Planet, Springer, pp 345-356, 2000.

[90] M. Morse, G. A. Hedlund, "Symbolic Dynamics," American Journal of Mathematics, vol. 60, pp. 815-866, 1938.

[91] M. Morse, G. A. Hedlund, "Symbolic Dynamics II, Sturmian Trajectories," American Journal of Mathematics, vol. 62, pp. 1-42, 1940.