Dynamical Systems Project

gunes akbas

May 2024

1 Introduction

Pseudo-random number generators are used in many areas such as engineering, especially modern cryptography. For cryptography generated random numbers carry an importance of how much good these random numbers are. We will informally talk about this issue. We aim to generate random numbers by chaotic dynamical systems and mathematically present proof about how random they are and the benefits of creating from a deterministic system.
First we need to give mathematical definitions for our setup:

Definition: A dynamical system may be defined formally as a measure-preserving transformation of a measure space, the triplet $(T, (S, \Sigma, \mu), \phi)$. Here, T is a monoid (usually the non-negative integers), S is a set, and (S, Σ, μ) is a probability space, meaning that Σ is a sigma-algebra on S and μ is a finite measure on (S, Σ). A map $\phi : T \times S \to S$ is said to be Σ-measurable if and only if, for every $A \in \Sigma$, one has

$$\phi^{-1}(A) \in \Sigma.$$

$\phi(n, s_0) = F(s_n)$, $n \in T$ and $s_0 \in S$
The trajectory starting from the initial state s_0 is the sequence $(s_n)_{n=0}^{\infty}$ of elements of S obtained by iteration

$$s_{n+1} = F(s_n), \quad n = 0, 1, 2, \ldots$$

Chaos

A dynamical system ϕ is chaotic on a compact invariant set X if ϕ is transitive and exhibits sensitive dependence on X.

Definition: A set $S \subset X$ is said to be *invariant* if $\phi_n(x) \in S$ for all $n \in \mathbb{N}$ whenever $x \in S$.

(This is the condition for chaos to restrict the states that can be exist inside and does not go outside.)

Definition: A flow ϕ exhibits sensitive dependence on an invariant set X if there is a fixed r such that for each $x \in X$ and any $\epsilon > 0$, there is a nearby $y \in B_\epsilon(x) \cap X$ such that $|\phi_n(x) - \phi_n(y)| > r$ for some $n \geq 0$.

(The dynamics of a system with sensitive dependence is difficult to predict: no matter how precisely an initial condition is specified, any small error may lead to a large one (at least of size r) after enough time. In other words, this condition is the popular example known as the butterfly effect.)

Definition: A dynamical system ϕ is topologically transitive on an invariant set X if for every pair of nonempty, open sets $U, V \subset X$, there is a $n > 0$ such that $\phi_n(U) \cap V \neq \emptyset$.

(This condition most generalized version of aperiodicity. In simpler terms, state space does not follow a periodic order)

Definition: A measurable transformation $F : S \to S$ is said to be measure preserving or to preserve μ, or alternatively, the measure μ is said to be F-invariant or invariant under F, if

$$\mu(F^{-1}(A)) = \mu(A), \quad \forall A \in \Sigma.$$

(Motivation for this mathematical definition can be explained by substitute as any measure to probability measure in the definition hence, transformation between same spaces preserves probabilities with that we understand that our dynamical system with this property events cause A equally likely to be A)

Definition: A measurable transformation F is said to be μ-ergodic or that μ is an ergodic measure for F if F preserves μ and the following condition holds:

$$\forall A \in \Sigma \text{ such that } F^{-1}(A) = A, \text{ either } \mu(A) = 0 \text{ or } \mu(A) = 1.$$

In other words, there are no F-invariant subsets up to measure 0 (with respect to μ).

(In mathematics, ergodicity expresses the idea that a point of a moving system, either a dynamical system or a stochastic process, will eventually visit all parts of the space that the system moves in, in a uniform and random sense.)

Definition: A dynamical system F is called mixing if the following condition is satisfied (for $\mu(S) = 1$):

$$\lim_{n\to\infty} \frac{\mu(F^{-n}(A) \cap B)}{\mu(B)} = \frac{\mu(A)}{\mu(S)}.$$

(Mixing implies ergodicity and like the name of it actually mixing stands for homogenity and two separate state spaces are mixing 'irreversibly' .)

Now we assumed that our discrete dynamical system F is:

1. F is chaotic dynamical system and,
2. F is mixing.

2 Forming Pseudo-random number generator

Now we will define a function that gives infinite binary sequence by our discrete dynamical system.To do this we divide state space into two equiprobable pieces.

$$G : S \to \prod_{i=1}^{\infty} \{0, 1\}$$

such that

$$G(s) = \{b_i(s)\}_{i=1,2,...} = \{b_1(s), b_2(s), \ldots\},$$

where $\prod_{i=1}^{\infty}\{0, 1\}$ is the Cartesian product of the infinite number of copies of the two-element set $\{0, 1\}$.
$b_n(s)$ is the n-th bit so

$$b_n(s) := \begin{cases} 1 & \text{if } \mathrm{F}^n(s) \in S_0 \\ 0 & \text{if } \mathrm{F}^n(s) \in S_1 \end{cases}$$

such that $\mu(S_0) = \mu(S_1) = 1/2, \quad \mathrm{s} \in S$, $\mathrm{S}_0 \cap S_1 = \emptyset \quad \text{and} \quad S_0 \cup S_1 = S$

3 Properties of Pseudo-Random number Generator

We will prove that for two different seeds in other words, two different initial points form completely different binary sequence.To show this we will prove that for any sequence generated probability with 0 because if density of any sequence more than 0 probability this means sequence can be generated by different initial conditions.

THEOREM 1: For two different seeds systems gives completely two different binary sequences:
For each $s \in S$ the following holds true:

$$\mu\left(G^{-1}\left(\{b_i(s)\}\right)\right) = 0.$$

Proof. Fix $s \in S$. Consider the sequence of bits

$$G(s) = \{b_1(s), b_2(s), b_3(s), \ldots, b_n(s), \ldots\}.$$

To simplify the notation we write further b_i instead of $b_i(s)$ and we introduce

$$S_{b_i} = S_0 \quad \text{for} \quad b_i = 0$$

and

$$S_{b_i} = S_1 \quad \text{for} \quad b_i = 1$$

Define the sets

$$A_{b_1} := F^{-1}\left(S_{b_1}\right),$$
$$A_{b_1 b_2} := F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right),$$

and, generally, $A_{b_1 b_2 \ldots b_n} \subset S, n = 3, 4, 5, \ldots,$

$$A_{b_1 b_2 \ldots b_n} := F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n}\left(S_{b_n}\right).$$

Observe that for every $n = 1, 2, \ldots, A_{b_1 b_2 \ldots b_n}$ is the set of all seeds z such that the first n initial bits of $G(z)$ are $(b_1, b_2, b_3, \ldots, b_n)$. More precisely,

$$z \in A_{b_1 b_2 \ldots b_n} \Longrightarrow b_i(z) = b_i(s), \quad \text{for} \quad i = 1, 2, \ldots, n.$$

This follows from the fact that for $i = 1, 2, \ldots, n$

$$F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n}\left(S_{b_n}\right) \subseteq F^{-i}\left(S_{b_i}\right),$$

and, consequently:

$$F^i(z) \in F^i\left(F^{-1}\left(S_{b_1}\right) \cap \ldots \cap F^{-n}\left(S_{b_n}\right)\right) \subseteq F^i\left(F^{-i}\left(S_{b_i}\right)\right) = S_{b_1} \equiv S_{b_s(s)},$$

which proves .

$$z \in A_{b_1 b_2 \ldots b_n} \Longrightarrow b_i(z) = b_i(s), \quad \text{for} \quad i = 1, 2, \ldots, n.$$

By the basic property of measure we have

$$\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n}\left(S_{b_n}\right)\right) \leq \mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-n}\left(S_{b_n}\right)\right).$$

Now we apply the mixing property to the two sets

$$F^{-1}\left(S_{b_1}\right) \text{ and } S_{b_n}$$

(the set S_{b_n} is equal to S_0 or S_1). For a given $\varepsilon > 0$ sufficiently small we choose n_1 such that

$$\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-n_1}\left(S_{b_{n_1}}\right)\right) \leq \mu\left(F^{-1}\left(S_{b_1}\right)\right) \mu\left(S_{b_{n_1}}\right) + \varepsilon.$$

Since μ is invariant, from above we obtain:

$$\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right)\right) \leq \mu\left(S_{b_1}\right) \mu\left(S_{b_{n_1}}\right) + \varepsilon.$$

Applying the mixing property (2.5) to the sets $A = S_{b_{n_2}}$, where

$$S_{b_{n_2}} = S_0 \quad \text{or} \quad S_{b_{n_2}} = S_1$$

for a certain $n_2 > n_1$, and

$$B = F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right),$$

and we have that if n_2 is sufficiently large then

$$\begin{aligned}
&\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right) \cap \ldots \cap F^{-n_2}\left(S_{b_{m_2}}\right)\right) \\
&\qquad \leq \mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right) \cap F^{-n_2}\left(S_{b_{m_2}}\right)\right) \\
&\qquad \leq \mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right)\right) \mu\left(F^{-n_2}\left(S_{b_{m_2}}\right)\right) + \varepsilon \\
&\qquad \leq \left[\mu\left(F^{-1}\left(S_{b_1}\right)\right) \mu\left(F^{-n_1}\left(S_{b_{n_1}}\right)\right) + \varepsilon\right] \mu\left(F^{-n_2}\left(S_{b_{n_2}}\right)\right) + \varepsilon
\end{aligned}$$

By the invariance property of the measure μ and the symmetry condition $\mu\left(S_0\right) = \mu\left(S_1\right) = 1/2$, we obtain the following inequality:

$$\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right) \cap \ldots \cap F^{-n_2}\left(S_{b_{n_2}}\right)\right) \leq \frac{1}{2}\left(\frac{1}{2} \cdot \frac{1}{2} + \varepsilon\right) + \varepsilon.$$

In general, using the complete induction property, we can find a sequence $\{n_1, \ldots, n_p\}$ for any p such that

$$\begin{aligned}
&\mu\left(A_{b_1 b_2 \ldots b_{n_1} \ldots b_{n_2} \ldots b_{n_p}}\right) := \\
&:= \mu\left(F^{-1}\left(S_{b_1}\right) \cap \ldots \cap F^{-n_1}\left(S_{b_{n_1}}\right) \cap \ldots \cap F^{-n_2}\left(S_{b_{n_2}}\right) \cap \ldots \cap F^{-n_F}\left(S_{b_{n_p}}\right)\right) \\
&\leq \left\{\left[\left(\mu\left(S_{b_1}\right) \mu\left(S_{b_{n_1}}\right) + \varepsilon\right) \mu\left(S_{b_{n_2}}\right) + \varepsilon \ldots\right] \mu\left(S_{b_{n_P}}\right) + \varepsilon\right\} + \varepsilon \\
&\leq \left\{\left[\left(\frac{1}{2} \cdot \frac{1}{2} + \varepsilon\right) \frac{1}{2} + \varepsilon \ldots\right] \frac{1}{2} + \varepsilon\right\} + \varepsilon.
\end{aligned}$$

We see that the right hand side of the above inequality is equal to the value of the n_p-th iteration of the function $h(x) = x/2 + \varepsilon$ at $x = 1/2$. For n_p sufficiently large, we have

$$h^{n_p}\left(\frac{1}{2}\right) < 3\varepsilon$$

Moreover, $A_{b_1 b_2 \ldots b_n} \subseteq A_{b_1 b_2 \ldots b_m}$ for every $n \leq m$ and

$$\mu\left(A_{b_1 b_2 \ldots b_n}\right) \leq \mu\left(A_{b_1 b_2 \ldots b_m}\right).$$

This means that the sequence of numbers $\mu\left(A_{b_1 b_2 \ldots b_n}\right), n = 1, 2, \ldots$ is monotonic and, since $\varepsilon > 0$ can be arbitrarily small, we deduce from last two expression with epsilon we understand that it contains a subsequence converging to zero. Thus,

$$\lim_{n \to \infty} \mu\left(A_{b_1 b_2 \ldots b_n}\right) = 0$$

THEOREM 2:By ergodicity frequency of 0 bits should equal to bits of 1's because we divide state space evenly. To be more precise, we can use the Birkhoff-Khinchin Ergodic Theorem , which applied to our system gives :

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \chi_{S_0} \left(F^i(s)\right) = \int_S \chi_{S_0} d\mu = \mu\left(S_0\right) = \frac{1}{2}$$

Birkhoff's pointwise ergodic theorem: Let (S, Σ, μ) be a measure space and let $F : (X, \Sigma, \mu) \to (X, \Sigma, \mu)$ be a measure-preserving transformation. Then, for each $f \in L^1(\mu)$, there exists a function $\tilde{f} \in L^1(\mu)$ such that $\tilde{f}(F(s)) = \tilde{f}(s), s \in S \quad \mu$-almost everywhere and

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} f\left(S^i(s)\right) = \tilde{f}(s), \forall s \in S \quad \mu\text{-almost everywhere.}$$

—Furthermore, if $\mu(S) < \infty$, then $\int_S \tilde{f}\ \mathrm{d}\mu = \int_S f\ \mathrm{d}\mu$.

4 Conclusion

We will extend and prove the uniformness of our generator function. One should talk about the usage of why chaotic systems. The answer is even though chaotic systems generate random numbers we can not reverse the process in other words information is lost in the process, our dynamical system is deterministic so it can be repeatable if the initial condition(seed) is known.

5 Materials and Methods

We mainly followed the article 'Pseudorandom Number Generators Based on Chaotic Dynamical Systems'.The proof above is taken in this article.

6 Resources

Differential Dynamical Systems-James D. Meiss
(Universitext) Jürgen Jost - Dynamical systems examples of complex behaviour-Springer (2005)
London Mathematical Society Student Texts
Mark Pollicott, Michiko Yuri - Dynamical Systems and Ergodic Theory (1998, Cambridge University Press)
Jiu Ding, Aihui Zhou - Statistical Properties of Deterministic Systems (Tsinghua University Texts)-Springer (2009)
https://en.wikipedia.org/wiki/Measure-preserving dynamical system