# Pseudo-Random Number Generator using Sinai Billiards

Dedicated to the memory of Maryam Mirzakhani

Advay Koranne

2019

**Abstract**

A novel method of generating pseudo-random numbers using Hamiltonian-Dynamical systems is presented in this paper. Using Sinai Billiards which exhibit chaotic non-periodic trajectories, I was able to create a pseudo random sequence. By enclosing a particle in a polygon with a convex disk in the center and simulating the collisions, I was able to generate a pseudo random sequence with a seed. This model can be implemented in photonics on a processor chip with scatterers, mirrors, and a laser as simulated through a particle on a billiard table. The applications for this are cryptography and the simulating of Lorentz gases. Computer simulation of the proposed method demonstrates the viability of such an approach on a Monte-Carlo problem. According to my research, this is the only known method for a non-periodic, pseudo-random number generator.

## Contents

# 1 Introduction

Using mathematical Billiards which is similar to the game of pool due to the enclosed polygon and a particle (ie. a pool ball), you can identity chaotic behavior of the particle. For example Sinai Billiards [5, 3] named after Yakov G. Sinai is modeled with a normal square billiards and a disk in the middle to increase chaotic behavior of the particles as shown in figure 1. Yakov G. Sinai proved a particle moving in a billiard is ergodic [1]. This chaotic behavior has many purposes and can be used in random number generators(RNG). There has been much progress over the years to determine which method for creating random numbers is the best; for example the NSA and Intel have worked together to create a chip which uses RdRand a natural way to find random numbers based of current. However, there are many benefits to have pseudo random numbers which are statistically random, as shown by their performance in the Monte-Carlo simulation and compares similarly to the Mersenne Twister algorithm [1] implemented by Julia language [2].

# 2 Problem Formulation

Determine whether using Sinai Billiards a computer chip is capable of modeling non-periodic, ergodic, pseudo-random numbers, using photonics.

Terms:

1. Billiards: A enclosed polygon ($\Omega$) with smooth edges ($\partial\Omega \in C^1$), no pockets, and friction less surface over which a particle of unit velocity is evolved with inelastic collisions [3],
2. Ergodic: Same behavior averaged over time, as over space,
3. Dense: In a given area every point is explored and covered or RNG numbers inclusive between 0 and 1 are explored. You can prove something is dense if it is ergodic,
4. Pseudo Random: Exhibit statistically randomness while being generated by using a seed, same seed generates the same sequence,
5. Deterministic: Method is reproducible and time evolution is predictable given initial conditions.

## 2.1 Simulation

The simulation was created using Julia's Dynamical Billiards. Using the package and open source software we were able to construct a hexagon and initiate it with a particle on the inside with a fixed velocity. [4].

[1] Ergodicity: In the case of billiards ergodicity means that in a given area every point is explored or covered. This also means for example that in a random number generator all numbers inclusive between 0 and 1 must be reachable

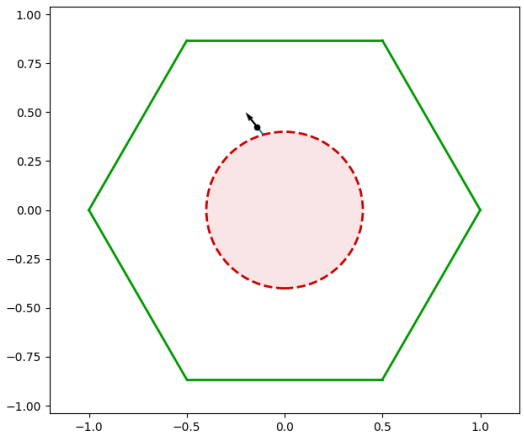


Figure 1: Sinai Billiard

### 2.2 Proof of Non-periodicity

Yakov G. Sinai proved a billiard moving a square table is ergodic [6].

## 3 Proposed Algorithm

Pseudo-random numbers have random number characteristics, however, when started with the same initial seed, they generate the same sequence. Prior to this research, no practical algorithm for generating non-periodic pseudo-random numbers was known. The seed in the proposed pRNG is the particle's initial location ($u_0$ in Birkhoff coordinate $\Gamma$) and velocity ($\theta$, as $|v| = 1$). The parameterization of the location of the particle from $(x, y) \in \partial\Omega$ to $\Gamma$ is one of the key ideas in my algorithm as that allows the map from $\Omega \to [0, 1]$ to be dense. Given this seed $(u_0, \theta) \in \Gamma \times 2\pi$ the time evolution $u(t), \theta(t)$ of the inelastic scattering generates the same sequence of numbers. It was one of the great discoveries of Sinai that although the system is integrable from initial conditions, almost all initial conditions exhibit non-periodic behavior, due to the scattering effect and positive Lyapunov exponent caused by the central disk. This non-periodicity makes our system future proof against attacks made by a much faster computer. Therefore, our pRNG can be used in cryptographic applications which have application life times spanning decades.

### 3.1 Advantages of proposed method

1. Fast (one number per clock cycle) especially when implemented on photonics due to short compute time,
2. State per pRNG is $u, \theta \in \Gamma \times 2\pi$: the same pRNG hardware can be shared to generate pRNGs for different applications. Each application only needs to store the particle location (in $\Gamma$) and velocity direction (as $\theta$),
3. Large list of batched pRNG computed in relatively short compute steps (batched RNGs are used in cryptography),
4. Mathematically proved infinite period: all other pRNG have periods, even when the period is $2^{32}$-bits, a fast computer in the future can break the cryptography.

Our algorithm is based on two fundamental mathematical principles, dynamical chaotic systems with positive Lyapunov exponents.

### 3.2 Lyapunov Exponent: $|u(t) - v(t)| \approx e^{\lambda t}|a(u_0 - v_0)|$

Lyapunov exponent $\lambda$ tells us the rate of divergence of nearby trajectories. Consider two particles $u, v$ with infinitesimally close initial positions $u_0, v_0$, and same $\theta$. Since our system has a Lyapunov exponent which is positive (due to the central disk) it is highly sensitive to changes, therefore for any given distance $M$ (less than the bounding diameter of the system), $\exists\, t$ such that $|u(t)-v(t)| > M$. This means that it is very hard to find the seed of a given sequence of numbers due to the exponential divergence of the paths.

### 3.3 Julia Simulation Process

Using the online documentation of Dynamical Billiards [4], we first created a hexagon with a internal disk. The length of each side of the hexagon was 1 unit. Then we initialized the billiard with a particle on the inside with a fixed velocity of 1 unit length per unit time. Then we created a random function which would evolve the particle n number of steps. Originally when we had done this we had taken the $60^{th}$ step of the particle. However, this method was not yielding a accurate value in the Mote-Carlo simulation. This was due to the fact that there were numerous areas where the particle was unable to reach certain values. The coordinates had to be dense.[2] Since the internal disk was unable reachable as well as the outside region between the hexagon and the square. To solve this issue we parametrized the boundary from 0 to 1 (Birkhoff coordinates). If there was no disc in the center of the polygon and their was a polygon the probability of a periodic function of time vs. location would be higher as supposed to having a central disk which would serve as a scatterer.

[2]Dense: This has the same meaning as ergodicity in billiards. If a polygon is dense it means that all points are explored and the table is covered

Consider a particle which hits the central disk and it scatters, then lets suppose the same particle goes parallel to the original trajectory except hits the disk a little lower, though the trajectory is only slightly different the particle will travel in a much different way due to the scattering effect of the disk.

### 3.4 Monte-Carlo Simulation

In order to determine whether the simulation had the properties of a true random generator we used the Monte Carlo Simulation. By finding the nth step of the particle and using the formula $x^2 + y^2 <= 1$ We were able to find all the points inside of the circle and outside as evident in figure 1.1. However, since random number generators on computers are only from 0 to 1 we restricted the domain to only the first quadrant and multiplied it by 4. We were also able to find all the points in the square and find the ratio which should have been fairly close to the value of $\pi$. We ran the same Monte-Carlo test on our chaotic billiards function as well as on Julia's and the values are shown below in the section 4.

## 4 Experimental Results

Using Julia's random number simulator and using my Monte Carlo Simulation for one trial the value was 3.14632 which is approximately -0.15047610977842357 % of from the actually value of $\pi$. Using the chaotic billiards simulation the value which we got was 3.14172 which was -0.004053562133881857 % of from the value of $\pi$. The Julia code was run on a Intel computer and the results are shown in Table 1

| Trials | Collisions | Julia Rand | Julia % Error | Our Rand | Our % Error |
|---|---|---|---|---|---|
| 10 | 10 | 2.0 | 36.338 | 2.8 | 10.8732 |
| 10 | 60 | 2.8 | 10.8732 | 3.6 | -14.5916 |
| 100 | 10 | 3.32 | -5.6789 | 2.8 | 10.8732 |
| 100 | 60 | 3.28 | -4.4056 | 2.88 | 8.3268 |
| 1000 | 10 | 3.152 | -0.3313 | 3.168 | -0.8406 |
| 1000 | 60 | 3.148 | -0.204 | 3.188 | -1.4772 |
| 10000 | 10 | 3.122 | 0.6237 | 3.1328 | 0.2799 |
| 10000 | 60 | 3.1616 | -0.6369 | 3.128 | 0.4327 |
| 100000 | 10 | 3.1274 | 0.4518 | 3.11848 | 0.7357 |
| 100000 | 60 | 3.1526 | -0.3504 | 3.14552 | -0.125 |

Table 1: Experimental results of Monte-Carlo $\pi$ estimation.

### 4.1 Numerical result of topological mixing

To prove topological mixing I calculated the number of times the particle entered a phase space of measure 1 (in Birkhoff coordinate) and the number of times a

| Topological Mixing | | |
|---|---|---|
| Trial | 2*Count (1 unit area) | Count (2 unit area) |
| 0 | 2 | 0 |
| 1 | 198 | 208 |
| 2 | 11764 | 11708 |
| 3 | 210474 | 209473 |
| 4 | 1951816 | 1956444 |
| 5 | 12097318 | 12090185 |

Table 2: Numerical simulation demonstrating topological mixing property of the proposed pRNG.

particle enters another phase space of twice measure. These second value should be approximately 2 times as much as the first if the particle is ergodic, and this is confirmed in the numerical simulation as shown above.

# 5 Conclusion

Recent vulnerabilities in computer architecture have demonstrated the need for future proof cryptographic hardware. Pseudo-random number generators can alleviate most of the known problems, but generating non-periodic pRNG has been an unsolved problem. This research presents the first practical and efficient method of generating non-periodic pRNG. Numerical experiments with Monte-Carlo applications demonstrate the efficacy of the method. As the algorithm derives its non-periodicity from well established mathematical methods of dynamical billiards, the cryptographic analysis of the technique is directly established. Advances in photonics and on-chip laser generation also imply that simulation of particle in billiards of a chaotic system can be done efficiently in hardware using photons. Though toady's pRNG have sufficiently long-periods ensuring security for data, as computer processing power doubles ever two years it is likely that future processors will be able to decrypt data easily. That is why it is is crucial to come up with a security element which has infinite period. Understanding polygon unfolding in higher dimensions using dynamical billiards is a future research goals which may lead to faster methods for pRNG generation.

# References


[1] Random numbers · the julia language. `https://docs.julialang.org/en/v1/stdlib/Random/index.html`. (Accessed on 02/15/2019).

[2] Jeff Bezanson, Alan Edelman, Stefan Karpinski, and Viral B Shah. Julia: A fresh approach to numerical computing. *SIAM review*, 59(1):65–98, 2017.

[3] Nikolai Chernov and Roberto Markarian. *Chaotic Billiards*. Number 127. American Mathematical Soc., 2006.

[4] George Datseris. DynamicalBilliards.jl: An easy-to-use, modular and extendable julia package for dynamical billiard systems in two dimensions. *The Journal of Open Source Software*, 2(19):458, nov 2017.

[5] Yakov G Sinai. Dynamical systems with elastic reflections. *Russian Mathematical Surveys*, 25(2):137–189, 1970.

[6] Serge Tabachnikov. *Geometry and billiards*, volume 30. American Mathematical Soc., 2005.