Stockholms
universitet

Analysing the Validity of Random Number Generators

Florian John

Kandidatuppsatsimatematiskstatistik
BachelorThesisinMathematicalStatistics

Kandidatuppsats 2023:12
Matematisk statistik
Juni 2023

www.math.su.se

Matematisk statistik
Matematiska institutionen
Stockholms universitet
106 91 Stockholm

Mathematical Statistics
Stockholm University
Bachelor Thesis **2023:12**
http://www.math.su.se

Analysing the Validity of Random Number Generators

Florian John[*]

June 2023

Abstract

In this thesis we aim to answer weather two popular pseudo random number generators can be considered random enough for their uses. We compare sequences from the pRNGs methods LCG and MT-19937 to one supposedly true random sequence and test different aspects of randomness such as goodness of fit measured using the Chisquare and Kolmogorov-Smirnov and independence which is tested using the Discrete Fourier transform test. The results show that the LCG failed the Discrete Fourier transform test and both the MT-19937 and the true random sequence did not fail a single test. We therefore consider the MT-19937 sufficiently random considering the fore-mentioned tests.

[*] Postal address: Mathematical Statistics, Stockholm University, SE-106 91, Sweden. E-mail: florian.john@hotmail.se. Supervisor: Mohamed El Khalifi Ola Gerton Henrik Hössjer.

Table of Contents

1 Introduction 3

2 Background 3

2.1 The concept of randomness 3

2.2 Random number generators 4

2.2.1 The Linear congruential generator 5

2.2.2 The Mersenne Twister method 5

2.3 True random numbers 5

2.4 Conversion methods 6

2.4.1 Binary to uniform conversion 6

2.4.2 Uniform to binary conversion 6

2.5 Statistical tests 6

2.5.1 The chisquare test for the marginal distribution 7

2.5.2 The Kolmogorov-Smirnov test for the marginal distribution 7

2.5.3 The spectral test for correlation structure 8

2.6 Applications of random number generators 10

3 Results 10

3.1 Chisquare tests 11

3.1.1 Goodness of fit test on uniform data 11

3.1.2 Chisquare test on binary data 11

3.2 Kolmogorov-Smirnov test 12

3.3 Spectral test 12

4 Conclusion 12

Acknowledgement

I want to thank my supervisors Mohamed El Khalifi and Ola Gerton Henrik Hössjer for their invaluable assistance and helpful input throughout the work on this thesis.

1 Introduction

Random number generators are used in many different applications, such as slot machines, statistical tests and simulations. The purpose of this study will be to determine if the variable randomness of these generators is sufficiently accurate to be used for such purposes. We start in section 2 by introducing such a definition of randomness for a sequence. A computer generating a truly random sequence purely based of programming is seen as an impossible task. A quote from a Professor of Computer Science and Engineering at MIT's Computer Science and Artificial Intelligence Laboratory, Steve Ward says that "On a completely deterministic machine you can't generate anything you could really call a random sequence of numbers, because the machine is following the same algorithm to generate them. Typically, that means it starts with a common 'seed' number and then follows a pattern."[2] Still we will present a more lenient definition of randomness which have criteria that may be fulfilled by an algorithm. After presenting a definition of randomness we proceed, in the following subsections, to introduce the Linear congruential (LCG) and Mersenne twister (MT-19937) random number generators, as well as values collected from the random.org website, which gather supposedly true random data from weather noise. Then later on in section 2 we describe conversion methods used to transform binomial random sequences to uniform random sequences, and vice versa. Following this in the same section we introduce the statistical tests used to test for randomness. We start by defining the chisquare test and the Kolmogorov-Smirnov test which are both used to test the null hypothesis that the marginal distribution of both samples follow a given distribution, mainly, the uniform distribution. The discrete Fourier transform test is then introduced and it tests the null hypothesis that the sequences contain values which are independent. Section 3 contains the results of the tests performed which can be viewed in four tables. In section 4 we conclude the report and consider the results which indicate that the MT-19937 RNG random number generator is sufficiently random while the LCG random number generator seems not to have independent values which is indicated by the failure of the Discrete Fourier transform test. Lastly, we present some conclusions in section 4.

2 Background

In this section we introduce the fundamental concepts in regards to random numbers and random number generators (RNGs), how they work, and what flaws they might have. And we introduce statistical methods for testing whether they are accurate or not.

2.1 The concept of randomness

In this thesis we will focus on the criteria of randomness and attempt to discuss whether different sequences satisfy these criteria.

From the two sequences 0101010101 and 0101100111 the first seems obviously non-random while the second appears random. In actuality the sequence on the left are just a sequence of alternating values while the sequence on the right are collected from supposedly true random values collected from random.org. This raises the question of what makes a sequence appear as random and non-random.

As we highlighted, true randomness is a concept which is difficult to define when applied to real data. But in in this section we will propose a definition that is the basis for testing randomness on real data later on.

A sequence of random variables $X_1, X_2, X_3, \ldots$ is said to be random if these random variables i) are independent and ii) all have the same marginal distribution function $F(x) = P(X_i \leq x)$ for $i = 1, 2, 3, \ldots$. This is usually referred to as the random variables being independent and identically distributed (i.i.d.).

In this thesis we will focus on two choices of the marginal distribution F. The first one is the uniform distribution $F \sim U(0, 1)$, whereby

$$F(x) = \begin{cases} 0; & x < 0, \\ x; & 0 \leq x \leq 1, \\ 1, & x > 1. \end{cases} \tag{1}$$

This is a continuous distribution with the probability density function

$$f(x) = \begin{cases} 1; & \text{for } \ x \in [0, 1], \\ 0; & \text{otherwise}. \end{cases} \tag{2}$$

When random numbers with a uniform distribution are used we often write $U_1, U_2, U_3, \ldots$ instead of $X_1, X_2, X_3, \ldots$.

The second option is binary random numbers, that correspond to a Bernoulli marginal distribution $F \sim \text{Be}(0.5)$. The corresponding distribution function is

$$F(x) = \begin{cases} 0; & x < 0, \\ 0.5; & 0 \leq x < 1, \\ 1, & x \geq 1. \end{cases} \tag{3}$$

This is a discrete distribution with $P(X_i = 0) = P(X_i = 1) = 0.5$.

2.2 Random number generators

In computer-science, simulations, entertainment and other applications random number generators (RNGs) are used to generate random values. Often times pseudo random number generators (pRNGs) are used since they are both fast and often accurate enough for their purpose. We will investigate two pRNGs in this thesis. They are referred to as the Linear congruential generator (LCT) and the Mersenne-Twister (MT-19937) methods respectively. To note in this thesis we will not be testing for other distributions such as random variables following a normal distribution (although this can be done by for example performing the inverse transformation method and transform the sequence of normally distributed random variables to uniform random variables). A known issue with

LCT and MT-19937 methods, and for any other pRNG, are their periodicity, meaning that the sequence of generated numbers will after a fixed length p repeat all previously generated numbers [7]. Let's now put our focus on the LCT and MT-19937 methods.

2.2.1 The Linear congruential generator

The Linear Congruential generator or LCG is a generator which was first presented by Derrick Henry Lehmer in 1951 as the Lehmer congruential generator [3], then revised by Kenneth Lane Thompson in 1958 [4]. In order to describe the method, let $h \bmod m \in \{0, 1, \ldots, m-1\}$ be the remainder when the integer h is divided by the positive integer m. The LCG creates an output using a starting seed $x_0 \in \{0, \ldots, m-1\}$ and a positive number a that is relatively prime to m. Then the algorithm

$$x_i = ax_{i-1} \bmod m,$$

for $i = 1, 2, 3, \ldots$ is utilized to create a series of integers $x_1, x_2, \ldots \in \{0, 1, \ldots, m-1\}$, and a corresponding sequence $U_i = x_i/m$ of pseudo random numbers with an approximate $U(0, 1)$ probability distribution [7]. This generator has been used extensively and is one of the more powerful generators with only a few disadvantages. One of those disadvantages will be discussed more thoroughly later in this thesis and it involves a dependency pattern which appears within the algorithm and that is detectable via a discrete Fourier transform test. The maximum period length, or how long the sequence can be before it repeats itself, is m.

2.2.2 The Mersenne Twister method

The Mersenne Twister algorithm was first proposed in 1998 and was based of the twisted generalised feedback shift register generator which will not be discussed in this thesis but is available to read in it's original thesis [6]. In this context the word "Mersenne" is a reference to the period length which is chosen to be the Mersenne prime $2^{19937}-1$. The algorithm is designed to generate uniform values with up to 32 bits accuracy and a period length $2^{19937} - 1$ [5]. Some notable properties that separate this algorithm from the LCG is the MT-19937's longer period length and slower generation speed.

2.3 True random numbers

The "true" random data was downloaded from random.org [9] in the form of binary-numbers $X_i \in \{0, 1\}$ with equal probabilities for each outcome, corresponding to the Bernoulli-distribution Be(0.5) in (3). Numbers were collected from all days in the month of January. The data was generated using three radios to pick up atmospheric noise that then was converted to random bits [10]. Combined for the entire month of January there were $n = 260\ 046\ 228$ observations. We will refer to this method as True random values or True rvs.

2.4 Conversion methods

In this section we will first describe a method for converting binary random variables to (approximately) uniform random variables. Then we will define a method that conversely transforms uniform random numbers to binary random numbers.

2.4.1 Binary to uniform conversion

We can convert binary values into continuous $U(0,1)$ using the following method.

Suppose we have a batch of k binary random variables $X_1, \dots, X_k$. If we regard them as the first k digits of a binary decimal expansion of a number between 0 and 1, this gives rise to a number

$$U = \sum_{i=1}^{k} X_i 2^{-i},$$

with a discrete uniform distribution on the 2^k points in $\{h/2^k;\ h = 0, 1, \dots, 2^k - 1\}$. When k is large it is clear that the distribution of U is close to $U(0,1)$.

Repeating this procedure n times, for disjoint collections of binary random numbers, we obtain a method for transforming nk binary random numbers to n approximate uniform random numbers.

We use this method with $k = 64$ in order to convert our true binary values into uniform ones which then has the sample size of $n = 260046228/64 \approx 4063222$ with 2^{-64} accuracy for the uniform distribution approximation.

2.4.2 Uniform to binary conversion

Suppose we have one single, uniformly distributed, random variable U. From this random variable it is possible to define m independent binary random variables $X_1, \dots, X_m$ as the first k digits of a binary decimal expansion of U. More formally we write this as

$$X_i = [2^i U] \bmod 2,$$

for $i = 1, \dots, k$, where $[x]$ is the integer part of x, whereas $h \bmod 2 \in \{0, 1\}$ refers to the remainder modulo 2 when dividing an integer h by 2.

Repeating this procedure for n independent and uniformly distributed random variables, we obtain from them nk binary random variables.

2.5 Statistical tests

For a given sequence $\{X_i\}_{i=1}^n$ of random variables of length n one might test randomness in various ways. In this section we will perform different statistical hypothesis tests, where some aspects of the randomness (i.i.d.) assumption are treated as a null hypothesis (H_0), whereas any departure from this null hypothesis is the alternative hypothesis H_a. Tests used in this thesis to detect randomness in sequences include the chisquare test, the Kolmogorov-Smirnov test, and the spectral test. We acknowledge that other tests can be used to detect randomness, however they were not considered in this thesis.

2.5.1 The chisquare test for the marginal distribution

The Pearson chi-square test is a statistical test which can be used to test goodness of fit for categorical data. The chisquare test may either be used for testing the marginal distribution or independence of a sequence of random variables. Here we will concentrate on testing the marginal distribution. Suppose we have n independent observations of a categorical variable with C categories $c = 0, \ldots, C-1$. Let O_c and $E_c = n\pi_c$ refer to the observed and expected number of observations that fall into category (or cell) c respectively. Here π_c is the probability that each observation equals c under the null hypothesis of a particular marginal distribution of the random sequence. The general expression for the chisquare test statistic is

$$T = \sum_{c=0}^{C-1} \frac{(O_c - E_c)^2}{E_c}, \tag{4}$$

and under the null hypothesis H_0, this test statistic approximately has a chisquare distribution with $C-1$ degrees of freedom ($T \sim \chi_{C-1}$) for large enough n. For an observed value t of the test statistic, the corresponding p-value is

$$p = P(\chi^2_{C-1} \geq t)$$

.

Now suppose we have a sequence $U_1, \ldots, U_n$ of n random variables and want to test whether the marginal distribution is uniform ($F \sim U(0,1)$), with F as in (1). For this purpose, divide the unit interval into C bins $B_c = (c, c+1)/C$ of equal length $1/C$, and let O_c refer to the number of U_i that fall into B_c for $c = 0, \ldots, C-1$. Under the null hypothesis of a uniform marginal distribution the probability of each bin is $\pi_c = 1/C$, so that $E_c = n/C$. Inserting these numbers into (4) we obtain the chisquare test statistic for testing a uniform marginal distribution of a random sequence.

On the other hand, for a sequence $X_1, \ldots, X_n$ of binary random numbers, we want to test whether the marginal distribution is Bernoulli with success probability 0.5 ($F \sim \mathrm{Be}(0.5)$), corresponding to equation (3). In this case we let each X_i be a categorical variable of the chisquare test, with $C = 2$ bins. This implies that O_c is the number of X_i with $X_i = c$. Moreover, under the null hypothesis we have that $\pi_0 = \pi_1 = 0.5$, and consequently $E_0 = E_1 = 0.5n$. If these numbers are inserted into (4) we obtain the chisquare test for binary random numbers.

2.5.2 The Kolmogorov-Smirnov test for the marginal distribution

The test checks if the empirical cumulative distribution function (ecdf) differs significantly from the expected theoretical cumulative distribution function (cdf) and this test may only be performed on continuous distributions. [8]. Emphasis in this test is on the shape of the assumed marginal distribution function of data. The Kolmogorov-Smirnov test does not require as large of a sample size as the chisquare test and can be performed directly on non-categorical data. The test is also a non parametric test in the sense that its test statistic has the same distribution under the null hypothesis regardless of which continuous marginal distribution that is being tested. We will only apply the KS test to test a uniform distribution, given a random sequence $U_1, \ldots, U_n \in [0,1]$ on the unit interval. In order to test the null hypothesis H_0 that the marginal distribution of $\{U_i\}$ is the uniform distribution (1), we define the empirical distribution function

$$F_n(x) = \frac{1}{n} \sum_{i=1}^{n} 1_{(U_i \le x)} \tag{5}$$

for all real-valued x. Note that $F_n(x)$ is the fraction of observations less or equal to x. Under the null hypothesis, F_n should be close to the uniform distribution function F in Eq.(1) for large n. The KS test statistic for testing H_0 is based on the re-scaled maximal distance between F_n and F, according to

$$T = \max_{-\infty < x < \infty} \sqrt{n} |F_n(x) - F(x)| = \max_{0 \le x \le 1} \sqrt{n} |F_n(x) - x|. \tag{6}$$

For large n we have approximately, under the null hypothesis, that

$$P(T \ge t | H_0) = 2 \sum_{h=1}^{\infty} (-1)^{h-1} e^{-2h^2 t}. \tag{7}$$

2.5.3 The spectral test for correlation structure

Unlike the chisquare and Kolmogorov-Smirnov (KS) tests we will see that The Discrete Fourier transform (spectral) test is a test for correlation which implies that the test provides information about correlation in a sequence of random numbers. The spectral test relies on the Fourier transform of the estimated covariance function, or equivalently the periodogram. The test is designed to detect periodic features that would otherwise remain undetected in other correlation tests, therefore it can be used to disprove randomness in linear congruental random number generators [13]. It is important to note that this is not the spectral test mentioned in Knuth [1] which plots a sequence $\{(X_t, \ldots, X_{t+d-1})\}_{t=1}^{n-d+1}$ in $d = 2$ or higher ($d > 2$) dimensions. Data from such plots form lines or hyperplanes, and compare the distance between these hyperplanes. Larger distances indicate worse generators.

The spectral test is based on the Discrete Fourier Transform. In order to define that test, suppose $X_1, \ldots, X_n$ is a sequence of independent and identically distributed random variables with a marginal distribution F, whose variance is

$$\sigma^2 = \int x^2 dF(x) - \left(\int x \, dF(x) \right)^2.$$

For instance, if a uniform marginal distribution $U(0,1)$ is assumed, then $\sigma^2 = 1/12$, whereas if a Bernoulli Be(0.5) marginal distribution is assumed, then $\sigma^2 = 1/4$.

Define the periodogram as

$$I_j = \frac{1}{n}|\sum_{t=1}^{n} X_t e^{-2\pi itj/n}|^2 = |D_j|^2/n,$$

for $j = 1, \cdots, n$, where i is the imaginary unit (a complex number), whereas D_j is the j:th component of the Discrete Fourier Transform (DFT) of $\{X_t\}_{t=1}^n$ at Fourier frequency $2\pi j/n$ [12]. Then, for large n, we have approximately that $I_1, \ldots, I_q$ are independent and exponentially distributed with mean $\sigma^2 = \text{Var}(X_t)$. This implies that approximately

$$P(I_j \leq x) = 1 - \exp(-x/\sigma^2) = G(x)$$

for $j = 1, \ldots, q$, with $\sigma^2 = 1/12$ for the $U(0,1)$ distribution and $\sigma^2 = 1/4$ for the Be(0.5)-distribution. In order to test the null hypothesis H_0 of $\{X_t\}_{t=1}^n$ being an independent and identically distributed sequence of random variables, we can therefore check how much the empirical distribution function

$$G_q(x) = \frac{1}{q}\sum_{j=1}^{q} 1(I_j \leq x)$$

of the periodogram departs from $G(x)$. This can be done in several ways. For the DFT test [13], the authors look at the distance between G_q and G at one point. More precisely, they introduce

$$T = \frac{\sqrt{q}(G_q(x) - G(x))}{\sqrt{0.95(1-0.95)}},$$

where $x = G^{-1}(0.95) = -\sigma^2 \log(0.05)$ is the 95% quantile of G. Under H_0 we have approximately for large n that $T \sim N(0,1)$ has a standard normal distribution. This gives rise to a p-value

$$p = P(|T| \geq t|H_0) = 2(1 - \Phi(t)) \tag{8}$$

for an observed value t of $|T|$, where Φ is the cumulative distribution function of a standard normal random variable $N(0,1)$. Formula (8) forms the basis of the DFT-test.

A more refined test of a DFT-based test is to calculate the maximal difference between G_q and G over all possible values of x, using the Kolmogorov-Smirnov test statistic

$$T = \max_{-\infty < x < \infty} \sqrt{q}|G_q(x) - G(x)|$$

Under H_0 we have that

$$P(T \geq t|H_0) = 2\sum_{h=1}^{\infty}(-1)^{h-1}e^{-2h^2t}, \tag{9}$$

which is also the p-value for an observed value t of T. See Brockwell and David (1991) [12] for more details and properties of the periodogram that underpins the DFT-test section and its generalization (9).

In this section we will perform the chisquare and Kolmogorov-Smirnov tests for goodness of fit for the uniform distribution and then the chisquare test for converted binomial values to check that they follow the hypothesized marginal distribution. Then we will also perform the spectral test in order to detect global frequency patterns. We will use the fast Fourier transformation which performs a discrete Fourier transformation of the sequence to the frequency domain as explained in [14].

2.6 Applications of random number generators

Since even before the invention of computers, the ability to generate randomly selected values has been invaluable. In modern times however the use for random values are many. But depending on their use, these random value need to meet different criteria for their generation, such as complexity(speed) and cryptographical security. In order to achieve this one may use different methods to generate pseudo random numbers or alternatively one may use hardware generated values. These may however have long generation time or be subject to other disadvantages. Services therefore exist where one may purchase or download supposedly accurate and true random values. An example of this is quantum random values which can be generated from fluctuations in the vacuum. Cryptographically secure values may be important for certain applications while not in others. One application that require highly cryptographically secure values are cryptocurrency transactions as well as token generations used to modify an access code. However, when applied commercially, the generator that was used is typically not revealed. It also of interest to mention that companies when marketing "true" random values often advertise these as a "cryptographically secure" option.

On the other hand when having low complexity is more important, one may instead choose to generate values using a method which can generate random values more rapidly. Examples where low complexity is important is in gambling machines, video-games and simulations. In simulations it is also of interest to be able to recreate a result by being able to use the same seed and method of generation, so that it is possible later on to get the same deterministic sequence of values as those that were generated originally.

3 Results

In this section we will perform the chisquare and Kolmogorov-Smirnov tests for goodness of fit for the uniform distribution and then the chisquare test for converted binomial values to check that they follow the hypothesized marginal distribution. Then we will also perform the spectral test in order to detect global frequency patterns. We will use the fast Fourier transformation which performs a discrete Fourier transformation of the sequence to the frequency domain and the method performed is available [14].

3.1 Chisquare tests

In this subsection we perform chi square tests for goodness of fit for our three data sources and their binary conversions.

3.1.1 Goodness of fit test on uniform data

For our three random samples LCG, MT-19937 and the true random data, we perform the chisquare test for the hypothesized marginal distribution.

In order to perform our goodness of fit test for uniform sequences we categorize our data into $C = 2\sqrt{n}$ bins where n is the sample size. This number of bins is chosen somewhat arbitrarily based of the optimal number of bins when testing goodness of fit for the normal distribution according to [15]. As mentioned in Section 2.1, we consider the following hypotheses

$$\begin{aligned} H_0 :&\quad \text{Data follow a uniform distribution,} \\ H_a :&\quad \text{Data do not follow a uniform distribution} \end{aligned} \tag{10}$$

Since the conversion to uniform from our true random binary data resulted in a sample of size of $n = 4063222$, in order to facilitate comparison we will use the same n for the two datasets constructed from pseudo random generators. This means that $C = 2\sqrt{n} = 4031.48$, or 4031 after rounding, which will then be our selected number of bins or categories.

Table 1: Chisquare goodness of fit test for uniform distribution with sample size + $n = 4063222$

Source	Statistic	p-value
LCG	65.63	1.0
MT-19937	4029.85	0.4977
True rvs	3986.08	0.6856

3.1.2 Chisquare test on binary data

Table 2: Chisquare goodness of fit test for the Bernoulli distribution Be(0.5), with sample size $n = 10^7$

Source	Statistic	p-value
LCG	0	0.9874
MT-19937	1.39	0.2382
True rvs	0.13	0.7147

3.2 Kolmogorov-Smirnov test

We now perform the KS test for goodness of fit for one sample with the null and alternative hypotheses as in (10). When performing KS test on a sample of the size $n = 4063222$ with continuous data in the interval $(0, 1)$, we get the results summarized in table 3.

Table 3: Kolmogorov-Smirnov goodness of fit test for the uniform probability distribution $U(0, 1)$ of sample size $n = 4063222$

Source	Statistic	p-value
LCG	$4.2232 \cdot 10^{-5}$	1.0000
MT-19937	$2.6494 \cdot 10^{-4}$	0.9379
True rvs	$3.4147 \cdot 10^{-4}$	0.7305

We observe that the LCG sample performs very well when tested with a p-value of 1, the MT-generated values performs well enough and the True random number generator performed similarly.

3.3 Spectral test

As we mentioned in section 2.5.3, the spectral test can be performed on binary data in order to test for global dependencies in our samples, and for this purpose we perform a discrete Fourier transform (spectral test) test. Recall from section 2.5.3 that our hypotheses are

$$\begin{aligned} H_0 &: \text{ Data is independent and indentically distributed,} \\ H_a &: \text{ Data is not independent and identically distributed.} \end{aligned}$$

We perform the spectral test for all three samples and report the results in table 4.

Table 4: The spectral test for binary sequences of sample size $n = 10^7$

Source	p-value
LCG	0
MT-19937	0.2410
True rvs	0.3699

From table 4 we observe that the LCG fails this test, while H_0 is not rejected for any of MT-19937 and True random values. More specifically, using a significance level of 5% we reject the null hypothesis that the LCG sample contain no global dependencies (since $p < 0.05$) while we do not reject H_0 both for MT-19937 and True random values.

4 Conclusion

The chisquare test and the KS test both resulted in our three samples of data on the unit interval appearing to have a marginal uniform distribution. Also our equivalent binary data samples also appeared uniform when tested on the chisquare test. We noted that for both of the two tests (chisquare and KS), the LCG sequence had a low test statistic value which is due to the fact that the deviation of the empirical marginal distribution from a uniform distribution for the LCG, is much smaller and thus outperforms the corresponding deviation for ”true” random numbers. It is notable that in this aspect of deviation from the shape of the uniform distribution the LCG ”outperforms” the supposedly ”true” random values. However, one might also argue that the marginal distribution of the LCG sequence is too close to a uniform distribution, since the p-values of the chisquare and KS-tests for the LCG sequence are very close to 1.

On the other hand, when performing the spectral test, we discovered that the LCG failed, whereas the MT-19937 and the true random data passed the test without rejecting the null hypothesis of independence. This indicates that as expected, dependencies in the LCG generated sequence were detected. According to our definition of randomness, mentioned in section 2.1, we note that the LCG sequence having dependencies means that its future values are more easily predictable. By our definition of randomness as ”independent and identically distributed”, this means that the LCG sequence is not random. Based on the tests performed, the MT-19937 algorithm appears to produce random data for a sequence of smaller length than its period. Since the sequence is deterministic, one could however predict values if the seed is known. This means that in that aspect the sample is non-random. Our ”true” random values pass all the criteria for randomness even though this sequence was ”outperformed” by the LCG method in terms of marginal distribution using either the KS or the chisquare test. Noting that the binary conversions did not affect the outcome of the tests for neither the chisquare test nor the spectral tests we conclude that the conversion did not introduce any deterministic patterns.

It is important to note that when testing for goodness of fit and independence one would ideally like to compute many $p-$values for each combination of test and method, based on many generated sequences. Then one could observe whether these p-values are uniformly distributed (by performing a chisquare test on these p-values) before drawing more definite conclusions. But due to time limitations this has not been performed in this thesis.

References

[1] Knuth, D. E. (1997). *The art of computer programming.* (2nd ed.). Addison Wesley.

[2] Rubin, J. M.(2011). Ask an engineer.
https://engineering.mit.edu/engage/ask-an-engineer/can-a-computer-generate-a-truly-random-number/

[3] Lehmer, D. H. (1951). Mathematical methods in large-scale computing units. *Proceedings of 2nd Symposium on Large-Scale Digital Calculating Machinery*

[4] Thomson, W. E. (1958). A Modified Congruence Method of Generating Pseudo-random Numbers" *The Computer Journal*, Volume 1, Issue 2, Page 83, https://doi.org/10.1093/comjnl/1.2.83

[5] Matsumoto, M. and Nishimura, T. (1998). Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generater, http://www.math.sci.hiroshima-u.ac.jp/m-mat/MT/ARTICLES/mt.pdf

[6] Matsumoto, M. and Kurita, Y. (1992). Twisted GFSR Generators, http://www.math.sci.hiroshima-u.ac.jp/m-mat/MT/ARTICLES/tgfsr3.pdf

[7] Hellekalek, P. (1998). *Mathematics and Computers in Simulation,* Good random number generators are (not so) easy to find, Volume 46, Issues 5–6, Pages 485-505, ISSN 0378-4754, https://doi.org/10.1016/S0378-4754(98)00078-0.

[8] NIST/SEMATECH, e-Handbook of Statistical Methods,

https://www.itl.nist.gov/div898/handbook/eda/section3/eda35g.htm

[9] Website containing random binary numbers generated from atmospheric noise, https://archive.random.org/binary

[10] Frequently asked question page on random.org, https://www.random.org/faq/Q1.4

[11] Stuart. G. R.(2015). Python package which performs the discrete Fourier transform test, https://gist.github.com/StuartGordonReid/54845bf66de7e195b335

[12] Brockwell, P.J. and Davis, R.A. (1991). *Time Series: Theory and Methods*, 2nd ed. Spinger Verlag, New York.

[13] Okada, H. and Umeno, H. (2017). Randomness evaluation of the Discrete Fourier Transform test based on exact analysis of the reference distribution. arXiv:1701.01960v1

[14] Rukhin. A, Soto. A, Nechvatal. J, Smid. M, Barker. E, Leigh. S, Levenson. M, Vangel. M, Banks. D, Heckert. N, Dray. J, Vo. S, Bassham. L, (2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

[15] White LF, Bonetti M and Pagano M. (2009) The Choice of the Number of Bins for the M Statistic. *Comput Stat Data Anal.* volume 53, issue 10, page 3640-3649. doi: 10.1016/j.csda.2009.03.005.