Annales Univ. Sci. Budapest., Sect. Comp. 55 (2023) 191–207

TEST OF MEASURES OF PSEUDORANDOM BINARY SEQUENCES

Károly Müllner (Budapest, Hungary)

Communicated by Imre Kátai

(Received May 30, 2023; accepted June 29, 2023)

Abstract. In the second half of the 1990's Christian Mauduit and András Sárközy introduced a new quantitative theory of pseudorandomness of binary sequences. Since then numerous papers have been written on this subject and the original theory was generalized in several directions. In this paper, I summarize some of the most notable results in the field. I compare four different constructions in the computational point of view. The first construction is the classic Legendre symbol construction, and the other three are construction based on digits of famous constants such as e, π, and $\sqrt{2}$. I used SAGE, PYTHON, and MATLAB as programming languages. I run multiple tests and calculated the exact values of the pseudorandom measures for each construction in many cases and the runtime are also presented.

1. Introduction

Among the pseudorandom measures defined by Christian Mauduit and András Sárközy, the well-distribution and a correlation measures are the most important. I give the definition of these measures in the second section.

The importance and strength of these measures are well illustrated by the fact that Rivat and Sárközy used a posteriori testing to study several sequences in construction based on the Legendre symbol. These were the a posteriori tests

Key words and phrases: Pseudorandomness, e, π,$\sqrt{2}$, Legendre symbol.
2010 Mathematics Subject Classification: 11K45.

contained in the ″1.4-sts. package″ created by the National Institute of Standards and Technology in the United States. Moreover, Rivat and Sárközy [13] proved that if the pseudorandom measures are small, the sequences "nearly" satisfy several of the above tests, and in this way some a posteriori testing can be avoided.

Many different construction with strong pseudorandom properties have been studied over the last 25 years. One of the strongest and most natural constructions to date is based on the Legendre symbol given by Hoffstein and Liemann:

$$E_p = \left(\left(\frac{f(1)}{p}\right), \left(\frac{f(2)}{p}\right), \left(\frac{f(3)}{p}\right), \dots \left(\frac{f(p)}{p}\right)\right)$$

construction, where $f(x) \in \mathbb{F}_p[x]$, which is not of the form $cg(x)^2$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$, but Hoffstein and Lieman have not provided evidence to support their claim that the above construction has strong pseudorandom properties. Goubin, Mauduit, and Sárközy proposed some simple conditions for the polynomial f if they were satisfied that the sequence has strong pseudorandom properties in the sense they defined.

The goal of this paper is to compare the well-distribution measure ($W(E_N)$), correlation measure ($C_2(E_N)$) and the Combined measure ($Q(E_N)$) in the case of four different constructions.

I have used different SAGE codes for calculating the binary digits of $\pi, e, \sqrt{2}$, than I had to convert all 0 digits to -1. This was solved by Python script. When we have the number of digits in the right format, it could be the inputs for MatLab source code which calculate the measure until 50000 digits.

2. Definition of the pseudorandom measures

In [14] Mauduit and Sárközy introduced the following pseudorandom measures in order to study the pseudorandom properties of finite binary sequences:

Definition 2.1. For a binary sequence $E_N = (e_1, e_2, \dots, e_N) \in \{-1, 1\}^N$ of lenght N, write

$$U(E_N, t, a, b) = \sum_{j=0}^{t} e_{a+jb}$$

Then the well-distribution measure of E_N is defined as

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=0}^{t} e_{a+jb} \right|$$

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le$ $\le a + tb \le N$.

The well-distribution measure studies how close are the frequencies of the $+1$'s and -1's in arithmetic progressions (for a binary sequence with strong pseudorandom properties these two quantities are expected to be very close.) But often it is also necessary to study the connections between certain elements of the sequence. For example, if the subsequence $(+1,+1)$ occurs much more frequently then the subsequence $(-1,-1)$, then it may cause problems in the applications, and we cannot say that our sequence has strong pseudorandom properties. In order to study connections of this type Mauduit and Sárközy [7] introduced the correlation and normality measures:

Definition 2.2. For a binary sequence $E_N = (e_1, e_2, \ldots, e_N) \in \{-1,1\}^N$ of lenght N, and for $D = (d_1, \ldots, d_l)$ with non-negative integers $0 \le d_1 \le \cdots \le d_l$, write

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l}.$$

Then the correlation measure of order to l of E_N is defined as

$$C_l(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} \right|,$$

where the maximum is taken over all $D = (d_1, d_2, \ldots, d_l)$ and M such that $0 \le d_1 < \cdots < d_l < M + d_l \le N$.

Definition 2.3. For a binary sequence $E_N = (e_1, e_2, \ldots, e_N) \in \{-1,1\}^N$ of lenght N, and for $X = (x_1, \ldots, x_l) \in \{-1,+1\}^l$ write

$$T(E_N, M, X) = |\{n : 0 \le n < M, (e_{n+1}, e_{n+2}, \ldots, e_{n+l})\}|.$$

Then the normality measure of order l of E_N is defined as

$$N_l(E_N) = \max_{M,X} \left| T(E_N, M, X) - M/2^l \right|,$$

where the maximum is taken over all $X = (x_1, \ldots, x_l) \in \{-1,+1\}^l$ and M such that $0 < M \ne N - l + 1$.

The combined (well-distribution-correlation) pseudorandom measure is a common generalization of the well-distribution and the correlation measures. This measure has an important role in the multidimensional extension of the theory of pseudorandomness.

Definition 2.4. For a binary sequence $E_N = (e_1, e_2, \ldots, e_N) \in \{-1,1\}^N$ of length N, and for $D = (d_1, \ldots, d_l)$ with non-negative integers $0 \le d_1 < \cdots < d_l$

$$Z(E_N, a, b, t, D) = \sum_{j=0}^{t} e_{a+jb+d_1} \cdots e_{a+jb+d_l}.$$

Then the combined (well-distribution-correlation) measure of order l of E_N is defined as

$$Q_l(E_N) = \max_{a,b,t,D} |Z(E_N, a, b, t, D)| = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} \cdots e_{a+jb+d_l} \right|,$$

where the maximum is taken over all a, b, t and $D = (d_1, ..., d_l)$ such that all the subscripts $a + jb + d_i$ belong to $\{1, 2, ..., N\}$.

When introducing their quantitative pseudorandom measures, the starting point of Mauduit and Sárközy was to balance the requirements possibly optimally. They decided to introduce functions which are real-valued and positive and the pseudorandom properties of the sequence are characterized by the sizes of the values of these functions. It was also an important requirement that one should be able to present constructions for which these measures can be estimated well. It turned out that the measures W and C_ℓ do not only satisfy these criteria, but later Rivat and Sárközy [13] showed that if the values of W and C_ℓ are "small", then the outcome of many (previously used a posteriori) statistical tests is guaranteed to be (nearly) positive.

We would like to use for testing "nice" sequences for pseudorandomness. This can be shown by an example, and indeed, we will test the Legendre symbol, which seems to be the the most natural candidate for pseudorandomness. The following construction and theorem is due to Mauduit and Sárközy [7]:

Construction 2.1. *Let p be an odd prime number, $N = p - 1$ and define the Legendre-sequence $E_N = (e_1, e_2, \dots e_N) \in \{-1, +1\}^N$ by*

$$e_n = \left(\frac{n}{p}\right),$$

where $\left(\frac{\div}{p}\right)$ denotes the Legendre symbol.

Theorem 2.1. *There is a number p_0 such that if $p > p_0$ is a prime number, $k \in \mathbb{N}$, $k < p$ and if we write*

$$E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots \left(\frac{p-1}{p}\right)\right)$$

then

$$Q_k(E_{p-1}) \le 9kp^{1/2} \log p$$

so that, writing $N = p - 1$

$$Q_k(E_N) = \max_{k \le (\log N)/\log 2} Q_k(E_N) \le 27N^{1/2}(\log N)^2$$

and also

$$Q_k^*(E_N) = \sum_{k=1}^{\infty} Q_k(E_N)/2^k \le 33N^{1/2}\log n$$

Then by above Theorem 2.1 for the sequence E_N defined in Construction 2.1 we have

$$W(E_N) \ll p^{1/2}\log p \ll N^{1/2}\log N \text{ and } C_l(E_N) \ll kp^{1/2}\log p \ll kN^{1/2}\log N.$$

Since then numerous binary sequence have been tested for pseudorandomness but still Construction 2.1 is the best (see also [14] for another construction which is just slightly worse).

3. Values of pseudorandom measures

Definition 3.1. A finite sequence $E_N = (e_1, e_2, \dots, e_N) \in \{-1, 1\}^N$ is said to be pseudorandom if for all $k \in \mathbb{N}$ with

$$k \le \frac{\log N}{\log 2} \tag{3.1}$$

and for all $X \in \{-1, 1\}^k$ we have

$$\left| T(E_N, N+1-k, X) - \frac{N+1-k}{2^k} \right| \le \sqrt{N}. \tag{3.2}$$

In [2] Cassaigne, Ferenczi, Mauduit, Rivat and Sárközy formulated the following principle: "The sequence E_N is considered a "good" pseudorandom sequence if these measures $W(E_N)$ and $C_\ell(E_N)$ (at least for "small" ℓ) are "small"." Indeed, the security of many cryptographic schemes is based on the property that the frequencies of the -1's and $+1$'s are about the same in certain "regular" subsequences of the used pseudorandom binary sequence $E_N \in \{-1, +1\}^N$.

In [3] Cassaigne, Mauduit and Sárközy proved that for the majority of the sequences $E_N \in \{-1, +1\}^N$ the measures $W(E_N)$ and $C_\ell(E_N)$ are around $N^{1/2}$ (up to some logarithmic factors):

Theorem 3.1. *Suppose that we choose each $E_N \in \{-1, +1\}^N$ with probability $\frac{1}{2^N}$. Then for all $\varepsilon > 0$ there are numbers $N_0 = N_0(\varepsilon)$ and $\delta = \delta(\varepsilon)$ such that for $N > N_0$ we have*

$$P\left(W(E_N) > \delta N^{1/2}\right) > 1 - \varepsilon \quad \text{and} \quad P\left(W(E_N) < 6\,(N\log N)^{1/2}\right) < \varepsilon.$$

Theorem 3.2. *Suppose that we choose each* $E_N \in \{-1,+1\}^N$ *with probability* $\frac{1}{2^N}$. *Then for all* $l \in \mathbb{N}, l > 2$ *and* $\varepsilon > 0$ *there are numbers* $N_0 = N_0(\varepsilon, l)$ *and* $\delta = \delta(\varepsilon, l)$ *such that for* $N > N_0$ *we have*

$$P\left(C_l(E_N) > \delta N^{1/2}\right) > 1-\varepsilon \quad \text{and} \quad P\left(C_l(E_N) < 5\left(lN\log N\right)^{1/2}\right) < \varepsilon.$$

First Kohayakawa, Mauduit, Moreira and Rödl [6], later Alon, Kohayakawa, Mauduit, Moreira and Rödl [1] sharpened these results.

In many applications it is enough to guarantiee that $W(E_N)$ and $C_l(E_N)$ are $O(N)$, but for the best constructions $E_N \in \{-1,+1\}^N$ it is proved that $W(E_N) << N^{1/2}\log N$, $C_l(E_N) << N^{1/2}(\log N)^{c_l}$.

We next state a result that establishes the typical order of magnitude of $C_k(E_N)$.

Theorem 3.3. *Let* $0 < \varepsilon_0 \le 1$ *be fixed and let* $\varepsilon_1 = \varepsilon_1(N) = (\log\log N)/\log N$. *There is a constant* $N_0 = N_0(\varepsilon_0)$ *such that if* $N \ge N_0$, *then, with probability at least* $1-\varepsilon_0$, *we have*

$$\begin{aligned}\frac{2}{5}\sqrt{N\log\binom{N}{k}} < C_k(E_N) \quad &< \quad \sqrt{(2+\varepsilon_1)N\log\left(N\binom{N}{k}\right)} < \\ &< \quad \sqrt{(3+\varepsilon_0)N\log\binom{N}{k}} < \frac{7}{4}\sqrt{N\log\binom{N}{k}}\end{aligned}$$

for every integer k *with* $2 \le k \le N/4$.

Theorem 3.4. *For any fixed constant* $\varepsilon > 0$ *and any integer function* $k = k(N)$ *with* $2 \le k \le \log N - \log\log N$, *there is a function* $\Gamma(k,N)$ *and a constant* N_0 *for which the following holds. If* $N \ge N_0$, *then the probability that*

$$1-\varepsilon < \frac{C_k(E_N)}{\Gamma(k,N)} < 1+\varepsilon$$

holds is at least $1-\varepsilon_0$.

Obviously Theorem 3.3 tells us that $\Gamma(k,N)$ is of order $\sqrt{N\log\binom{N}{k}}$. The proof can be found in [6].

4. Results of tests and runtime analysis

Following that, I will discuss my own results. Taking the first N binary digits of well-known constants (in our case, π, e, and $\sqrt{2}$) are some of the most

basic pseudorandom constructions. This results in N-long binary sequence in each cases. In this section, I compare the pseudorandom measures of the three constructions created this manner and the Legendre symbol-based one for different N's. Our constructions are the following:

Construction 4.1. *Let $c \in \{e, \pi, \sqrt{2}\}$, the binary digits expansion of c is $c = c_1c_2c_3\ldots$. Define $E_N(c) = \{e_1, e_2, \ldots e_N\}$ by*

$$e_i = \begin{cases} 1 & \text{if } c_i = 1 \\ -1 & \text{if } c_i = 0 \end{cases}$$

The last construction is the Legendre symbol construction(see Construction 2.1)

4.1. Results for π

In the table below, we have summarized the running results for different digits lengths. We can see the running times in seconds and hours, as well as the different measures for each digit. Furthermore, in the last column of the table, we also calculated the upper limit as a function of N, which we learned in Theorem 3.3. The obtained data were represented in a common figure, where two types of upper limits were presented. One is the mentioned Theorem 3.3 (upper bound 1) that is $\frac{7}{4}\sqrt{N \cdot \log\binom{N}{k}}$, the other limit (upper bound 2) elliminates the factor $\frac{7}{4}$, that is $\sqrt{N \cdot \log\binom{N}{k}}$

digits(N)	runtime(s)	runtime(h)	$W(E_N)$	$C_2(E_N)$	$\frac{7}{4} \cdot \sqrt{N \cdot \log\binom{N}{2}}$
200	0.7078	0	43	35	77.875
1000	28.61	0.008	59	100	200.375
2000	98	0.027	68	153	298.095
5000	902.5	0.25	116	253	500.220
7500	1095	0.30	129	309	627.660
10000	2296.8	0.638	142	399	736.820
12500	2655	0.73	142	455	834.100
15000	3763	1.04	142	474	922.820
17500	4952	1.37	142	523	1005.020
20000	11884	3.3	142	559	1081.990

We conjecture that $W(E)$ is monotonic because the obtained measures increase with the length of the digits. As the table shows, repeated values are possible. For example, from 10000 to 20000, we got 142, but after running additional tests (e.g. for 30000 digits), we get 205. As a result, the well-distribution measure is monotonic but not strictly monotonic.

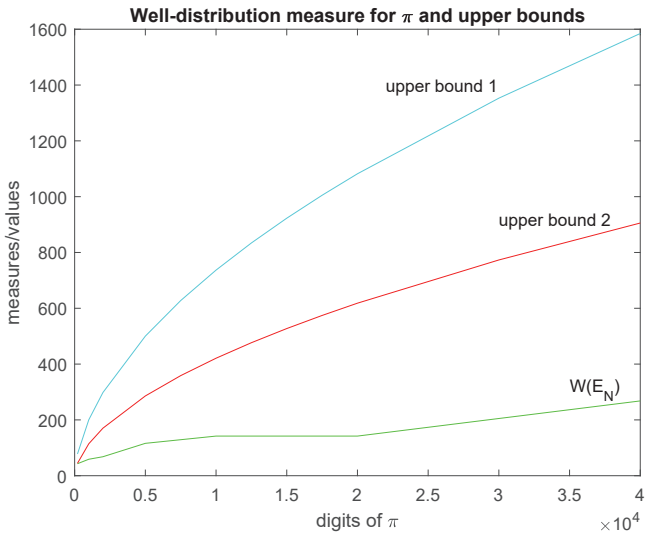

Figure 1. Well-distribution measures and upper bounds for π

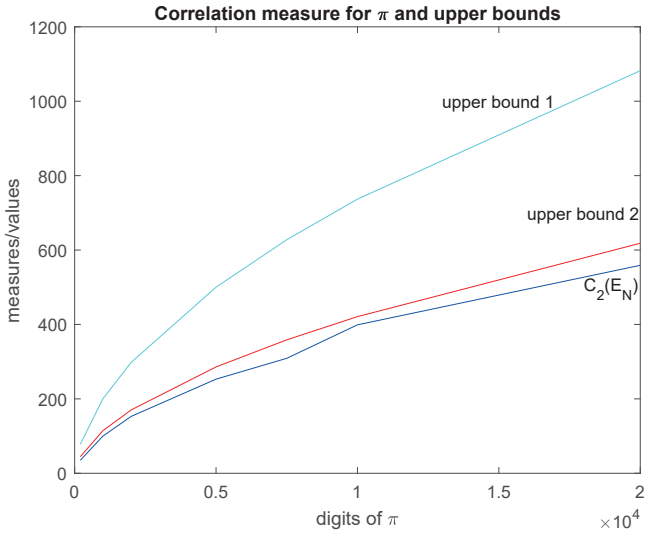

Figure 2. Correlation measures and upper bounds for π

4.2. Results for e

digits(N)	runtime(s)	runtime(h)	$W(E_N)$	$C_2(E_N)$	$\frac{7}{4}\cdot\sqrt{N\cdot\log\binom{N}{k}}$
200	1.7	0.0005	13	41	77.87
1000	61.306	0.017	66	99	200.37
2000	269.75	0.075	105	162	298.09
5000	1232.11	0.3422	180	251	500.22
7500	988	0.27	180	314	627.66
10000	4445.13	1.234	180	399	736.82
12500	5247	1.45	180	445	834.10
15000	5481	1.52	180	452	922.82
17500	5760	1.6	180	534	1005.02
20000	19091	5.3	180	568	1081.99

We frequently get the same measure for digits of different lengths. In case of e we got the same value (180) from 5000 up to 30000. But it does not stay that way forever, because it eventually changes, e.g. we get $W(E) = 213$ at $N = 40000$ digits. These repetitions can be seen only in the well-distribution measure but the correlation measures give a different value for each length.

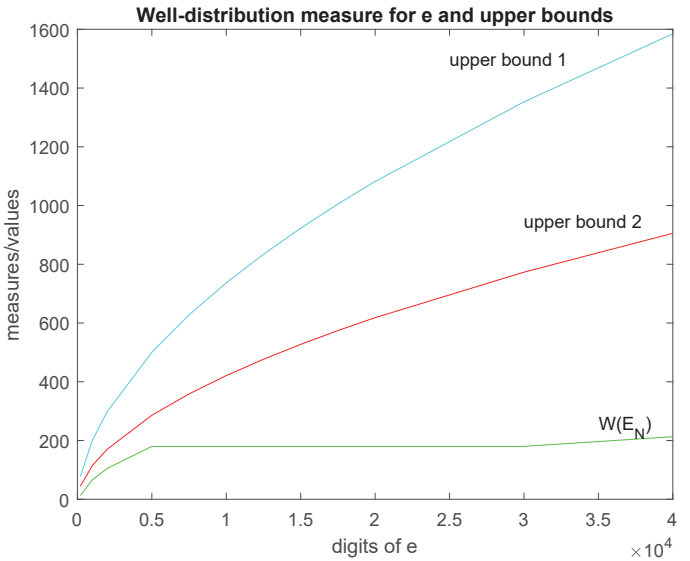

Figure 3. Well-distribution measures and upper bounds for e

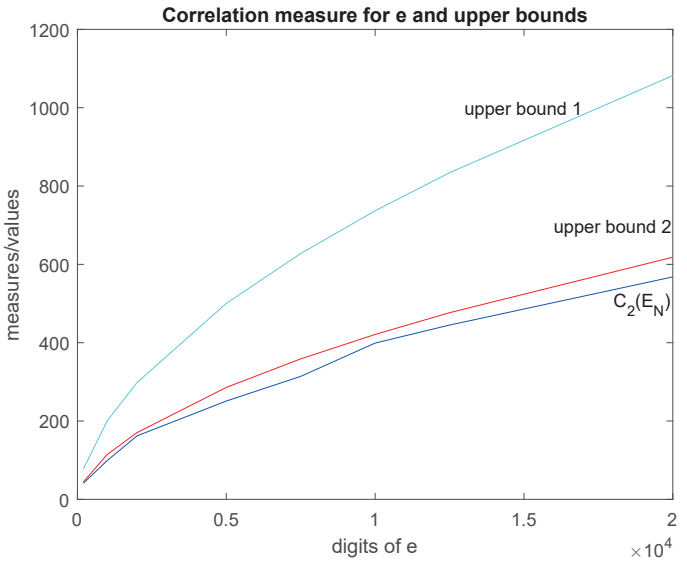

Figure 4. Correlation measures and upper bounds for e

4.3. Results for $\sqrt{2}$

In the case of $\sqrt{2}$, we found a case where the upper bound 2 was below the calculated correlation measure($C_2(E_{2000}) = 173$) for $N = 2000$ digits. Upper bound 1 is $\frac{7}{4}\sqrt{N \log \binom{N}{k}}$ and upper bound 2 is $\sqrt{N \log \binom{N}{k}}$.

digits(N)	runtime(s)	runtime(h)	$W(E_N)$	$C_2(E_N)$	upper_b_2	upper_b_1
200	1.31	0.0004	23	38	44.50	77.87
1000	46.9	0.013	50	89	114.50	200.37
2000	200	0.06	82	173	170.34	298.09
5000	1627	0.45	112	247	285.84	500.22
7500	892	0.25	112	329	358.66	627.66
10000	2240	0.62	148	359	421.04	736.82
12500	2655	0.73	148	481	476.62	834.08
15000	3763	1.04	148	492	527.32	922.82
17500	4952	1.37	197	513	574.28	1005.02
20000	9468	2.63	197	547	618.28	1081.99

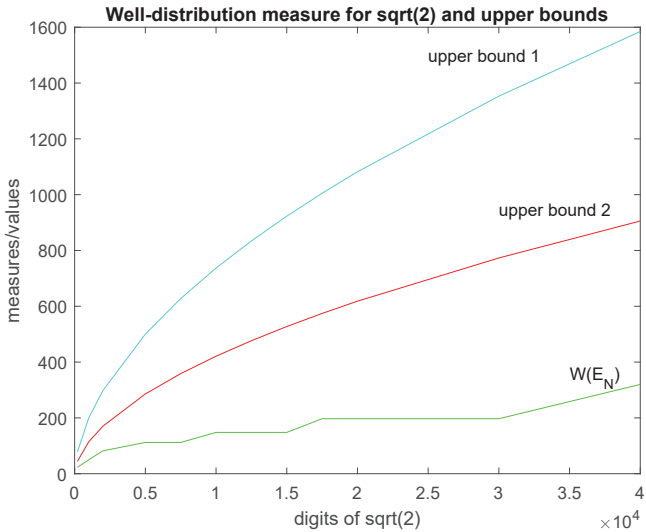

Figure 5. Well-distribution measures and upper bounds for $\sqrt{2}$

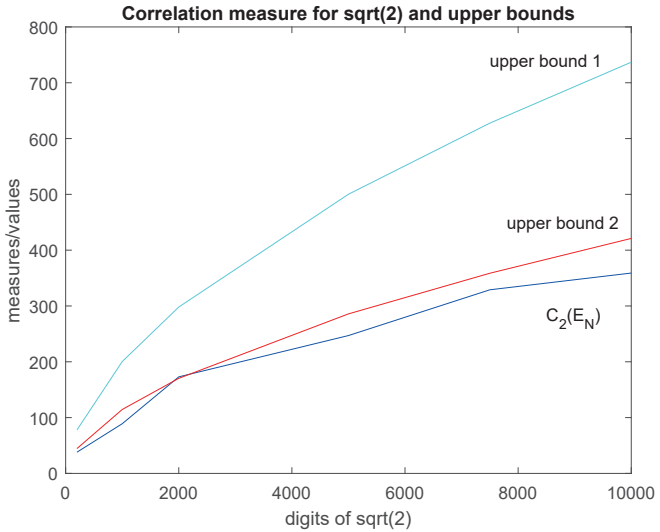

Figure 6. Correlation measures and upper bounds for $\sqrt{2}$

It is clearly visible in the figure that the upper_bound 2 is also above the obtained measures in all other cases.

4.4. Results for Legendre symbol

In the case of the Legendre symbol, we obtained the smallest measures for both well-distribution and correlation measures, in this case the upper bound 2 can be used as an upper limit. Because we intended to test the Legendre symbol on a similar sample size, we chose a prime greater than the necessary sample size and applied the $N = p - 1$ relationship. (see Construction 2.1)

digits(N)	runtime(s)	runtime(h)	$W(E_N)$	$C_2(E_N)$	$\sqrt{N \cdot \log \binom{N}{2}}$
210	0.7	0.00	18	29	45.82
1008	19	0.00	36	68	115.07
2002	103	0.03	50	100	170.44
5002	572	0.16	78	159	285.90
7506	1129	0.31	99	211	358.82
10006	2605	0.72	130	227	421.18
12502	8958	2.49	124	260	476.66
15012	12081	3.36	174	315	527.56
17508	16132	4.48	164	320	574.44
20010	8949	2.48	158	337	618.45

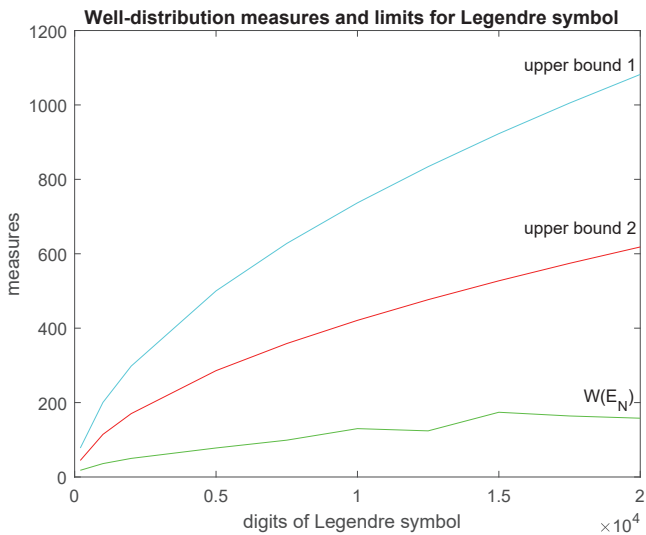

Figure 7. Measures and upper bounds for Legendre symbol

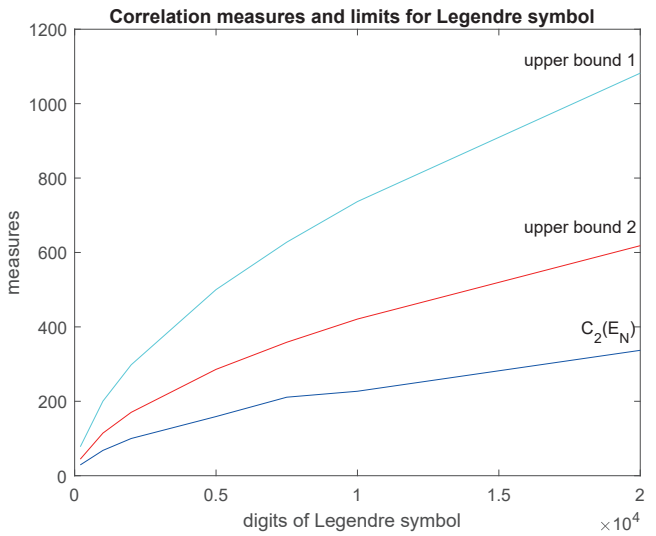

Figure 8. Correlation measures and limits for Legendre symbol

5. Comparison of the results

In the table below, we have summarized the well-distribution and correlation measures obtained for the digits of various irrational numbers. It is clear, especially as we increase the digits, that we get the smallest values (measures) for the Legendre symbol. Indeed based on our tests the Legendre symbol seems to be the most natural candidate for pseudorandomness.

5.1. Values of well-distribution measures

Measure	Legendre symbol	π	e	$\sqrt{2}$
$W(E_{200})$	18	43	13	23
$W(E_{1000})$	36	59	66	50
$W(E_{2000})$	50	68	105	82
$W(E_{5000})$	78	116	180	112
$W(E_{7500})$	99	129	180	112
$W(E_{10000})$	130	142	180	148
$W(E_{12500})$	124	142	180	148
$W(E_{15000})$	174	142	180	148
$W(E_{17500})$	164	142	180	197
$W(E_{20000})$	158	142	180	197
$W(E_{30000})$	196	205	180	197
$W(E_{40000})$	236	268	213	320

As shown in the table above

1. $2.39 \cdot W_{Legendre} \geq W_c$ for $c \in \{e, \pi, \sqrt{2}\}$ in all cases.
2. $1.65 \cdot W_{Legendre} \geq W_c$ for $c \in \{\pi, \sqrt{2}\}$, if $N \geq 1000$.

In the second case as the sample size increases, the constant multiplier starts to decrease (but not monotonically).

- $E = 1000$, const.= 1.65
- $E = 2000$, const.= 1.64
- $E = 5000$, const.= 1.49
- $E = 7500$, const.= 1.31
- $E = 10000$, const.= 1.14
- $E = 12500$, const.= 1.2
- $E = 15000$, const.= 0.85
- $E = 17500$, const.= 1.21
- $E = 20000$, const.= 1.25
- $E = 30000$, const.= 1.05
- $E = 40000$, const.= 1.36

5.2. Values of correlation measures

Measure	Legendre symbol	π	e	$\sqrt{2}$
$C_2(E_{200})$	29	35	41	38
$C_2(E_{1000})$	68	100	99	89
$C_2(E_{2000})$	100	153	162	173
$C_2(E_{5000})$	159	253	251	247
$C_2(E_{7500})$	211	309	314	329
$C_2(E_{10000})$	227	450	399	359
$C_2(E_{12500})$	260	455	445	481
$C_2(E_{15000})$	315	474	452	492
$C_2(E_{17500})$	320	523	534	513
$C_2(E_{20000})$	337	559	568	547

As shown in the table above

1. $2 \cdot C_{2,Legendre} \geq C_{2,d}$ for $d \in \{e, \pi, \sqrt{2}\}$, in all cases.
2. $1.76 \cdot C_{2,Legendre}$ is always greater than the measures of e.

6. SW source codes

6.1. SAGE and CoCalc

For generate thousands of digits of irrational number in base 2 we can use Sage CoCalc project online page (https://cocalc.com/). The following code generates 50000 digits of e and convert it to base 2.

```
R=RealField(50000); R
R(e).str(base=2)
```

6.2. Python

The outputs of Sage will be the input for Python code what is able to modify the sequence in order to change all 0 to -1 and insert a comma between each digits. We need this format due to vector base MatLab source code. For further references see the [8].

6.3. MatLab code - calculate well-distribution measure

See the MatLab source code in GitHub site which calculates the well-distribution measure [9]

6.4. MatLab code - calculate correlation measure

See the MatLab source code in GitHub site which calculates the correlation measure [10]

6.5. MatLab code - calculate Legendre symbol

See the MatLab source codes in GitHub site which calculate the well-distribution measure [11] and the correlation measure for Legendre symbol [12].

References

[1] **Alon, N., Y. Kohoyakawa, C. Mauduit, C.G. Moreira and V. Rödl,** Measures of pseudorandomness for finite sequences: minimal values, *Combinatorics, Probability and Computing*, **15(1-2)** (2006), 1–29.

[2] **Cassaigne, J., S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy,** On finite pseudorandom binary sequences III: The Liouville function, I, *Acta Arith.*, **87** (1999), 367–384.

[3] **Cassaigne, J., C. Mauduit and A. Sárközy,** On finite pseudorandom binary sequences VII: The measures of pseudorandomness, *Acta Arith.*, **103** (2002), 97–118.

[4] **Goubin, L., C. Mauduit and A. Sárközy,** Construction of large families of pseudorandom binary sequences *Journal of Number Theory*, **106** (2004), 56–69.

[5] **Gyarmati, K. and C. Mauduit,** On the correlation of binary sequences, II, *Discrete Math.*, **312** (2012), 811–818.

[6] **Kohoyakawa, Y., C. Mauduit, C.G. Moreira and V. Rödl,** *Measures of pseudorandomness for finite sequences: Minimum and typical values*, 2003. https://www.researchgate.net/publication/228575895

[7] **Mauduit, C. and A. Sárközy,** On finite pseudorandom binary sequence I: Measure of pseudorandomness, the Legendre symbol, *Acta Arithmetica*, **82(4)** (1997), 365–377.

[8] **Müllner, K.,** Python code for create the right format of sequences https://github.com/mullni/Test_of_measures_of_pseudo_seq/blob/main/convert_text_file.py

[9] **Müllner, K.,** MATLAB code for calculate well-distribution measure https://github.com/mullni/Test_of_measures_of_pseudo_seq/blob/main/well_distribution_measure.m

[10] **Müllner, K.,** MATLAB code for calculate correlation measure
https://github.com/mullni/Test_of_measures_of_pseudo_seq/blob/main/correlation_measure.m

[11] **Müllner, K.,** MATLAB code for calculate well-distribution measure of Legendre-symbol
https://github.com/mullni/Test_of_measures_of_pseudo_seq/blob/main/Legendre_measures.m

[12] **Müllner, K.,** MATLAB code for calculate correlation measure of Legendre symbol
https://github.com/mullni/Test_of_measures_of_pseudo_seq/blob/main/Legendre_Correlation_measures.m

[13] **Rivat, J. and A. Sárközy,** On pseudorandom sequences and their application, *Lecture Notes in Comput. Sci. 4123, General theory of information transfer and combinatorics, Springer, Berlin / Heidelberg*, (2006), 343–361.

[14] **Sárközy, A.,** A finite pseudorandom binary sequence, *Studia Sci. Math. Hungar.*, **38** (2001), 377–384.

K. Müllner
Eötvös Loránd University
Institute of Mathematics
H-1117 Budapest Pázmány Péter sétány 1/C
Hungary
mullni@hotmail.com