A Horadam-based Pseudo-random Number Generator

Ovidiu D. Bagdasar
School of Computing and Mathematics
University of Derby
Derby, UK
Email: o.bagdasar@derby.ac.uk

Minsi Chen
School of Computing and Mathematics
University of Derby
Derby, UK
Email: m.chen@derby.ac.uk

***Abstract*—Uniformly distributed pseudo-random number generators are commonly used in certain numerical algorithms and simulations. In this article a random number generation algorithm based on the geometric properties of complex Horadam sequences was investigated. For certain parameters, the sequence exhibited uniformity in the distribution of arguments. This feature was exploited to design a pseudo-random number generator which was evaluated using Monte Carlo π estimations, and found to perform comparatively with commonly used generators like Multiplicative Lagged Fibonacci and the 'twister' Mersenne.**

***Keywords*-Random number generation; Horadam sequence; simulation; Monte Carlo methods; linear recurrence**

I. Introduction

A random number generator is a core component of numerical algorithms based on simulation and statistical sampling. For example, Monte Carlo methods are widely used for numerically solving integrals. In such applications, it is desirable to have a random sequence that closely resembles the underlying differential equations. The current implementations of pseudo-random number generator are based on classical methods including *Linear Congruences* and *Lagged Fibonacci Sequences* [12].

In this paper, we will discuss and evaluate the properties of a random generator based on Horadam sequences. Our examination focused on the following requirements [11]:

- Period
- Uniformity
- Correlation

The Fibonacci numbers are the members of the integer sequence $1, 1, 2, 3, 5, 8, 13, 21, 34, ...$ obeying the rule that each subsequent element is the sum of the previous two. These numbers are ubiquitous in nature (flower and fruit patterns or bee crawling) and play a role arts, science or...stock exchange [8, Chapter 3]. The Fibonacci numbers can be defined by the recurrence

$$F_{n+2} = F_{n+1} + F_n, \quad F_0 = 1, F_1 = 1, \tag{1}$$

and the general term is given by $F_n = (\phi^n - \phi^{-n})/\sqrt{5}$, where $\phi = \frac{1+\sqrt{5}}{2} \approx 1.61803\,39887\cdots$ is the golden ratio (sequence A001622 in OEIS).

The Horadam sequence $\{w_n\}_{n=0}^{\infty}$ is a natural extension of the Fibonacci sequence [7], defined by the recurrence

$$w_{n+2} = pw_{n+1} + qw_n, \quad w_0 = a, w_1 = b, \tag{2}$$

where the parameters a, b, p and q are complex numbers (an important property of the Horadam sequence is therefore that its terms can be actually visualized in the complex plane). For particular values of the parameters a, b, p and q one obtains the Fibonacci sequence for $(a, b) = (0, 1)$ and $(p, q) = (1, -1)$ and the Lucas sequence for $(a, b) = (0, 1)$ and $(p, q) = (1, 1)$. Some results related to Horadam sequences are given in the survey of Larcombe *et al.* [9].

The characterization of periodic Horadam sequences was done in [1], the results being formulated in terms of the initial conditions a, b and the generators z_1 and z_2 representing the roots (distinct or equal) of the quadratic characteristic polynomial of the recurrence (2)

$$P(x) = x^2 - px + q. \tag{3}$$

Vieta's relations for the polynomial P give

$$p = z_1 + z_2, \quad q = z_1 z_2, \tag{4}$$

showing that the recurrence (2) defined for the coefficients p, q may alternately be defined through the solutions z_1, z_2 of the characteristic polynomial, referred to as *generators*. The periodicity of the Horadam sequence is equivalent with z_1 and z_2 being distinct roots of unity, denoted by $z_1 = e^{2\pi i p_1/k_1}$ and $z_2 = e^{2\pi i p_2/k_2}$ where p_1, p_2, k_1, k_2 are natural numbers. A classification of the geometric patterns produced by periodic Horadam sequences was proposed in [2]. The Horadam sequences with a given period have been enumerated in [3], which gave the first enumerative context and asymptotic analysis for the O.E.I.S. sequence no. A102309.

In this paper, aperiodic Horadam sequences will be shown to densely cover prescribed regions in the complex plane, while producing a uniform distribution of the arguments in the interval $[-\pi, \pi]$. This property is used to evaluate π, along with classical pseudo-random number generators.

II. METHODOLOGY

In this section are presented the formulae for the general term w_n of the complex Horadam sequence having the characteristic polynomial (3), inner and outer boundaries of periodic or stable orbits, as well as the structure of degenerate orbits. The computations and graphs in this paper were realized using Matlab®.

A. Properties of general Horadam sequences

For distinct roots $z_1 \neq z_2$ of (3), the general term of Horadam's sequence $\{w_n\}_{n=0}^{\infty}$ is given by [5, Chapter 1]

$$w_n = Az_1^n + Bz_2^n, \tag{5}$$

where the constants A and B can be obtained from the initial conditions $w_0 = a$ and $w_1 = b$.

Geometric boundaries for the periodic Horadam sequences are specified in [1, Theorem 4.1], in terms of the generators z_1,z_2 and the parameters

$$A = \frac{az_2 - b}{z_2 - z_1}, \quad B = \frac{b - az_1}{z_2 - z_1}. \tag{6}$$

The periodic orbit is located inside the annulus

$$\{z \in \mathbb{C} : |\,|A| - |B|\,| \leq |z| \leq |A| + |B|\}. \tag{7}$$

The notations $S = S(0;1)$, $U = U(0;1)$ and $U(0;r_1,r_2)$ are used for the unit circle, unit disc, and annulus of radii r_1 and r_2 centered in the origin.

For $z = re^{2\pi ix}$ and $r = 1$, the orbit of $\{z^n\}_{n=0}^{\infty}$ is a regular k-gon if $x = j/k \in \mathbb{Q}$, $\gcd(j,k) = 1$, or a dense (and uniformly distributed) subset of S, if $x \in \mathbb{R}\setminus\mathbb{Q}$. For $r < 1$ or $r > 1$, one obtains inward, or outward spirals, respectively. The orbits of Horadam sequences given by (5), are linear combinations of the sequences $\{z_1^n\}_{n=0}^{\infty}$ and $\{z_2^n\}_{n=0}^{\infty}$ for certain generators z_1, z_2 and coefficients A and B [1].

B. Dense Horadam orbits

Certain bounded orbits are dense within a circle or an annulus centered in the origin. Specifically, if $r_1 = r_2 = 1$ and the generators $z_1 = e^{2\pi ix_1} \neq z_2 = e^{2\pi ix_2}$ satisfy the relation $x_2 = x_1 q$ with $x_1, x_2, q \in \mathbb{R} \setminus \mathbb{Q}$, then the orbit of the Horadam sequence $\{w_n\}_{n=0}^{\infty}$ is dense in the annulus $U(0, |\,|A| - |B|\,|, |A| + |B|)$, as one can see in Fig. 1.

The parameters are $r_1 = r_2 = 1, x_1 = \frac{\sqrt{2}}{3}, x_2 = \frac{\sqrt{5}}{15}$ and $a = 2 + \frac{2}{3}i$, $b = 3 + i$. These types of dense orbits are here examined and used to design a random number generator.

III. RESULTS AND DISCUSSION

Below we examine the periodicity, uniformity and autocorrelation for the arguments of terms of sequence $\{w_n\}_{n=0}^{\infty}$ defined by (5) for initial conditions $w_0 = a$, $w_1 = b$, in the particular case $|A| = |B|$. In this instance, sequence terms are all located within a circle of radius $2|A|$, as in Fig. 2.

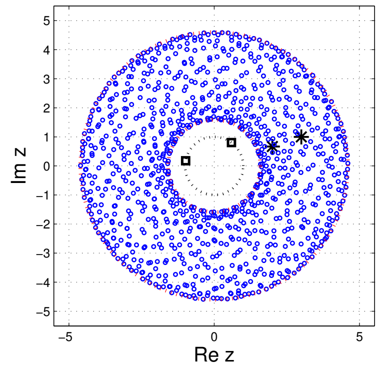


Fig. 1. First 1000 terms of the sequence $\{w_n\}_{n=0}^{\infty}$ obtained from (5). Stars represent the initial conditions w_0, w_1, squares the generators z_1, z_2 and the dotted line the unit circle. The dotted circles represent the boundaries of the annulus $U(0, |\,|A| - |B|\,|, |A| + |B|)$.

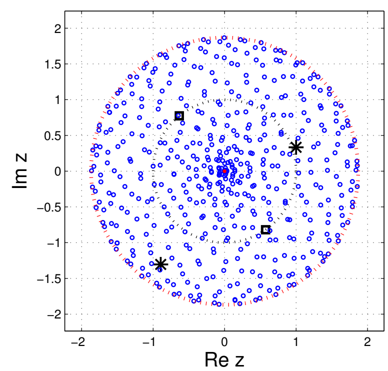


Fig. 2. First 500 terms of sequence $\{w_n\}_{n=0}^{\infty}$ from (5). Stars represent the initial conditions w_0, w_1, squares the generators z_1, z_2 and the dotted line the unit circle. The dotted circle is $U(0,\, 2|A|)$.

In Figs 2, 3, 4, the parameters are $r_1 = r_2 = 1$, $x_1 = \exp(1)/2, x_2 = \exp(2)/4$ and $a = 1 + 1/3i$, $b = 1.5a\exp(\pi(x_1 + x_2))$.

It is known that for an irrational number θ, the sequence $\{n\theta\}_1^{\infty}$ is equidistributed $\mod 1$ (Weyl's criterion). This property represents the basis for a novel random number generator, which is used to evaluate the value of π.

A. Argument of Horadam sequence terms

If $A = R_1 e^{i\phi_1}, B = R_2 e^{i\phi_2}, z_1 = e^{2\pi ix_1}, z_2 = e^{2\pi ix_2}$, the nth Horadam term w_n in polar form is given by

$$re^{i\theta} = Az_1^n + Bz_2^n = R_1 e^{i(\phi_1 + 2\pi nx_1)} + R_2 e^{i(\phi_2 + 2\pi nx_2)}. \tag{8}$$

Denoting $\theta_1 = \phi_1 + nx_2, \theta_2 = \phi_2 + nx_2$, one can write

$$re^{i\theta} = R_1 e^{i\theta_1} + R_2 e^{i\theta_2}, \quad \theta_1, \theta_2 \in \mathbb{R}, \quad R_1, R_2 > 0, \tag{9}$$

where R_1, R_2 are positive and θ_1 and θ_2 are real numbers. For $R = R_1 = R_2$, the formula for θ gives

$$\theta = \frac{1}{2}(\theta_1 + \theta_2). \tag{10}$$

B. *Periodicity of arguments*

From (10), the sequence of arguments for w_n is

$$\theta_n = \frac{\phi_1 + \phi_2}{2} + 2\pi n(x_1 + x_2). \tag{11}$$

For irrational and algebraically uncorrelated values x_1, x_2, $x_1 + x_2$ is also irrational, so the sequence of arguments θ_n is aperiodic. This property is also valid for the sequence of normalised arguments $(\theta_n + \pi)/(2\pi)$.

C. *Uniform distribution of arguments*

The sequence of arguments produced by certain Horadam sequences is uniformly distributed in the interval $[-\pi, \pi]$.

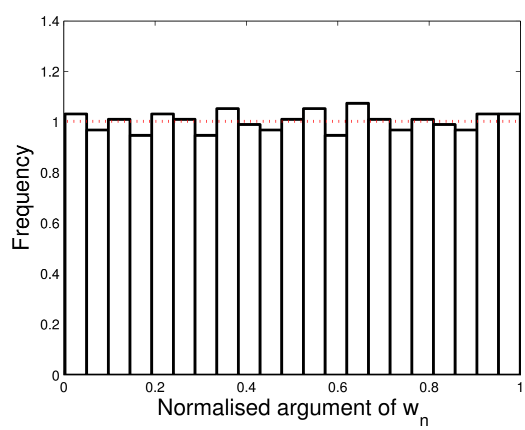


Fig. 3. Histogram of $\frac{\arg(w_n)+\pi}{2\pi}$ vs uniform density on $[0, 1]$.

When the values of x_1 and x_2 are irrational, the arguments $\theta_1 = \phi_1 + 2\pi n x_2, \theta_2 = \phi_2 + 2\pi n x_2 \in [-\pi, \pi]$ are uniformly distributed modulo 2π. This guarantees that θ is uniformly distributed on $[-\pi, \pi]$. The normalised argument $(\theta + \pi)/(2\pi)$ is then uniformly distributed in $[0, 1]$ (Fig. 3).

D. *Autocorrelation of arguments*

A test for the quality of pseudo-random number generators is the autocorrelation test [11]. For a good quality generator, the 2D diagrams of normalised arguments (θ_n, θ_{n+1}) should uniformly cover the unit square. The plot depicted in Fig. 4 suggests that consecutive arguments are very correlated.

This issue can be addressed in several ways. One of them is combining arguments produced by two distinct Horadam sequences, the other using generalised Horadam orbits.

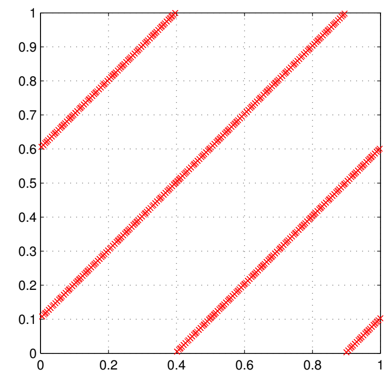


Fig. 4. Normalized angle correlations: $(\text{Arg}(w_n), \text{Arg}(w_{n+1}))$.

E. *Mixed arguments and Monte Carlo based methods*

The purpose of this simulation was to test the performance of the uniform distribution of normalized Horadam angles as a pseudo-random number generator. Here we evaluate the Horadam-based method against classical methods like the Multiplicative Lagged Fibonacci and the Mersenne Twister pseudo-random number generators implemented in Matlab (the latter is the default random number generator).

A Monte Carlo simulation approximating the value of π could involve randomly selecting points $(x_n, y_n)_{n=1}^N$ in the unit square and determining the ratio $\rho = m/N$, where m is number of points that satisfy $x_n^2 + y_n^2 \leq 1$. In our simulation two Horadam sequences $\{w_n^1\}$ and $\{w_n^2\}$ computed from formula (5) are used.

The parameters are $x_1 = \frac{e}{2}, x_2 = \frac{e^2}{4}$ for $\{w_n^1\}$, and $x_1 = \frac{e}{10}, x_2 = \frac{\pi}{10}$ for $\{w_n^2\}$, while the initial conditions satisfy $a = 1 + \frac{1}{3}i$, $b = 1.5a\exp(\pi(x_1 + x_2))$. The 2D coordinates plotted in Fig. 5 represent normalized arguments of Horadam sequence terms, given by the formula

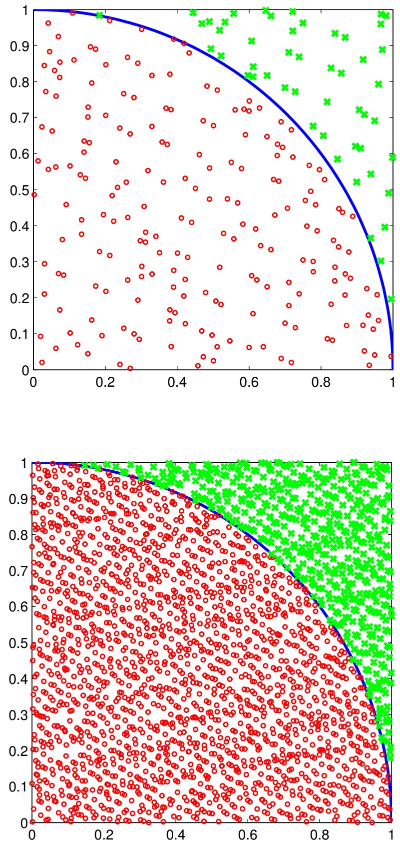
$$(x_n, y_n) = \left(\frac{\text{Arg}(w_n^1) + \pi}{2\pi}, \frac{\text{Arg}(w_n^2) + \pi}{2\pi}\right). \tag{12}$$

In the simulation shown in Fig. 5(a), the sample size is $N = 1000$ and there are 792 points satisfying $x_n^2 + y_n^2 \leq 1$. Using this data, one obtains

$$\rho = \frac{792}{1000} = 0.792 \text{ and } \pi \sim 4\rho = 3.1680. \tag{13}$$

The approximation significantly improves with the increase in the number of sequence terms, to 3.1420 for $N = 10^4$ (depicted in Fig. 5 (b)) and to 3.141888 for $N = 10^6$.

A more detailed illustration of this convergence is shown in Table I. Sequences H1 and H2 represent simulations for π obtained from pairs of Horadam sequences. In particular, H1 was obtained from sequences w_n^1 and w_n^2, while H2 from



(a)

(b)

Fig. 5. First (a) 1000; (b) 10000 points (x_n, y_n) (12). Also represented, points inside (circles) and outside (crosses) the unit circle (solid line).

TABLE I
10^N IS THE SAMPLE SIZE USED IN EACH SIMULATION.

10^N	H1	H2	F1	F2	MT1	MT2
1	0.0584	0.0584	-0.3297	-0.3297	-0.7258	0.8584
2	0.2584	-0.0216	0.0985	-0.0615	-0.0215	0.0985
3	0.0784	-0.0016	-0.0136	0.0304	-0.0456	0.0264
4	0.0104	0.0004	0.0092	-0.0200	0.0036	0.0096
5	0.0012	-0.0006	-0.0016	-0.0018	0.0004	-0.0034
6	0.0003	0.0000	-0.0001	-0.0010	-0.0026	-0.0015
7	0.0000	0.0000	0.0003	-0.0006	-0.0002	0.0004

sequences w_n^1 and w_n^3 given below by (x_1, x_2, a, b).

$$w_n^1 : \left(\frac{e}{2}, \frac{e^2}{4}, 1 + \frac{1}{3}i, 1.5ae^{\pi(x_1+x_2)}\right) \tag{14}$$

$$w_n^2 : \left(\frac{e}{10}, \frac{\sqrt{5}}{15}, 1 + \frac{2}{3}i, 1.5ae^{\pi(x_1+x_2)}\right) \tag{15}$$

$$w_n^3 : \left(\frac{\sqrt{2}}{3}, \frac{e}{15}, 1 + \frac{2}{3}i, 1.5ae^{\pi(x_1+x_2)}\right) \tag{16}$$

The 2D coordinates producing the results in the table are then given by the formulae

$$\text{H1}: \quad (x_n, y_n) = \left(\frac{\text{Arg}(w_n^1) + \pi}{2\pi}, \frac{\text{Arg}(w_n^2) + \pi}{2\pi}\right), \tag{17}$$

$$\text{H2}: \quad (x_n, y_n) = \left(\frac{\text{Arg}(w_n^1) + \pi}{2\pi}, \frac{\text{Arg}(w_n^3) + \pi}{2\pi}\right). \tag{18}$$

The sequences F1, F2 are each produced using two coordinates (x_n, y_n) simulated by the 'multFibonacci' Multiplicative Lagged Fibonacci pseudo-random generator. The generator for F1 had a periodicity of 2^{31} whilst the one for F2 was 2^{16}. This produced a noticeable difference in the convergence rate.

The sequences MT1, MT2 are each produced using two coordinates (x_n, y_n) simulated by the 'twister' Mersenne Twister pseudo-random generator. Both MT1 and MT2 used the default seed value as implemented in Matlab.

It is noticeable that the convergence is non-monotonic for all methods, although it appears more rapid for our Horadam based generator. This is dependent on the choice of initial parameters. Further examination is needed to fully describe the relationship between seeds and the convergence rate.

IV. Conclusion and Future Work

A. *Results obtained so far*

We have shown that random numbers generated from Horadam sequences of arbitrary order exhibit angular uniformity in the complex plane. In the case of second order linear aperiodic case, for certain value of the initial parameters we were able to estimate the value of π with a precision and a convergence rate comparable to the more classical pseudo-random number generators.

B. *Generalised Horadam sequences*

One direction for generalizing and improving the results in this paper is by using generalised Horadam sequences, produced by higher order recurrences. For three distinct generators $z_1 = r_1 e^{2\pi i x_1}$, $z_2 = r_2 e^{2\pi i x_2}$ and $z_3 = r_3 e^{2\pi i x_3}$ and initial values a_1, a_2, a_3 the general term of Horadam's sequence $\{w_n\}_{n=0}^{\infty}$ is given by

$$w_n = Az_1^n + Bz_2^n + Cz_3^n, \tag{19}$$

where the constants A, B and C can be obtained from the initial conditions $w_0 = a_1$, $w_1 = a_2$ and $w_2 = a_3$. A sequence obtained for $r_1 = r_2 = r_3 = 1$, $x_1 = \sqrt{2}/2$, $x_2 = \sqrt{3}/2$, $x_3 = \sqrt{5}/6$ and $a_1 = 0.2e^{2\pi/7+\pi/3}, a_2 = 0.4e^{2\pi 3/7+\pi/3}, a_3 = 0.8e^{2\pi 5/7+\pi/3}$, is illustrated in Fig. 6.

Generalised Horadam arguments appear to be uniformly distributed. The autocorrelation plot obtained for normalised arguments (θ_n, θ_{n+1}) depicted in Fig. 7 suggests that the performance of Horadam-based pseudo-random number generators may improve by increasing the order of the recurrence. The investigation is currently in progress.

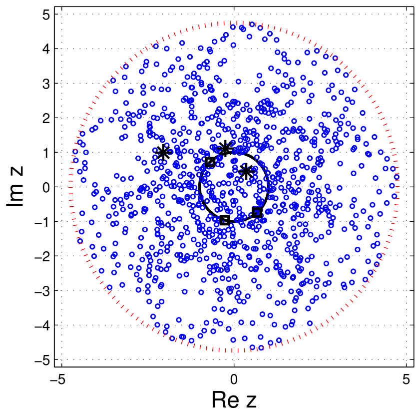


Fig. 6. First 1000 terms of the sequence $\{w_n\}_{n=0}^{\infty}$. Stars represent the initial conditions w_0, w_1, w_3, squares the generators z_1, z_2, z_3 and the dotted line the unit circle.

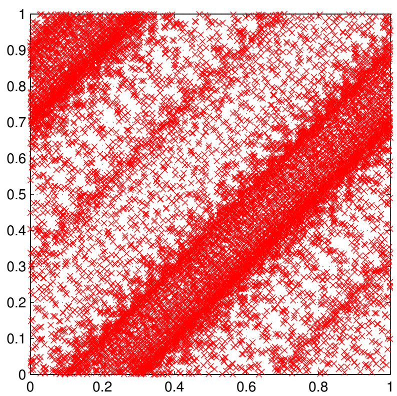


Fig. 7. 2D correlation of normalized arguments of $\{w_n\}_{n=0}^{\infty}$.

C. Limitations

Under the constraint of machine floating point precision, the sequence of arguments eventually becomes periodic. We are able to circumvent this issue by using long-periodic Horadam sequences investigated in [3].

REFERENCES

[1] Bagdasar, O. and Larcombe, P. J., *On the characterization of periodic complex Horadam sequences,* Fibonacci Quart. vol.51, no.1, 28–37 (2013)

[2] Bagdasar, O., Larcombe, P. J., and Anjum, A., *Geometric patterns of periodic complex Horadam sequences and applications,* Submitted to Appl.Math.Comp.

[3] Bagdasar, O., Larcombe, P. J.: *On the number of complex Horadam sequences with a fixed period*, Fibonacci Quart., vol.51, no.4, 339–347 (2013)

[4] Coxeter, H. S. M., Introduction to Geometry, New York Wiley (2nd Ed.) (1969)

[5] Everest, G., Poorten, A., Shparlinski, I. and Ward, T., Recurrence Sequences, Mathematical Surveys and Monographs, Volume 104, 318 pp (2003)

[6] Graham, I. and Kohr, G., Geometric Function Theory in One and Higher Dimensions, Marcel Dekker Inc, New York, 530 pp (2003)

[7] Horadam, A. F., *Basic properties of a certain generalized sequence of numbers,* Fibonacci Quart. **3**: 161–176 (1965)

[8] Koshy, T., Fibonacci and Lucas Numbers with Applications, John Wiley & Sons, Inc., Hoboken, NJ, USA (2001)

[9] Larcombe, P. J., Bagdasar, O. D., Fennessey, E. J.: *Horadam sequences: a survey*, Bulletin of the I.C.A., **67**, 49–72 (2013)

[10] Latapy, M., Phan, T.H.D., Crespelle, C., Nguyen, T.Q., *Termination of Multipartite Graph Series Arising from Complex Network Modelling,* Combinatorial Optimization and Applications, Lecture Notes in Computer Science, Volume 6508, pp 1-10 (2010)

[11] Hellekalek, P. *Good random number generators are (not so) easy to find,* Mathematics and Computers in Simulation, vol.46, pp 485-505 (1998)

[12] Oohama, Y. *Performance analysis of the internal algorithm for random number generation based on number systems* IEEE Trans. on Information Theory, vol.57, no.3, pp 1177-1185 (2011)