2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Pseudo Random numbers generated by Dynamical Systems

Makoto Mori

Department of Mathematics, College of Humanities Sciences, Nihon University
3–25–40 Sakura Jyosui, Setagayaku, Tokyo 156-8550, Japan
Email: mori@math.chs.nihon-u.ac.jp

Abstract—One of the most important pseudo random numbers is a van der Corput sequence. We will consider it from the view point of dynamical systems, and show that the discrepancy of pseudo random numbers is deeply connected with the ergodicity of a dynamical system. We first study 1–dimensional cases, and then construct higher dimensional transformations which generate low discrepancy sequences. Main tools are the spectra of Perron–Frobenius operator and renewal equations.

1. Introduction

Let $I = [0,1]^d$ ($d \geq 1$) and $F\colon I \to I$. We consider a partition $\{\langle a\rangle\colon a \in \mathcal{A}\}$ of I, and express (I, F) to a symbolic dynamics. Let X be a set of infinite sequences of symbols $a_1 a_2 \cdots$ ($a_i \in \mathcal{A}$), such that $\bigcap_{i=1}^{\infty} F^{-i+1}(\langle a_i\rangle)$ consists of unique point. We assume a dynamical system X with the shift is isomorphic to (I, F).

We denote a finite sequence of symbols $a_1 \cdots a_n$ ($a_i \in \mathcal{A}$) a word and

- $|w| = n$,
- $\langle w\rangle = \bigcap_{i=1}^{n} F^{-i+1}(\langle a_i\rangle)$,
- for $x \in I$, wx is a point such that $wx \in \langle w\rangle$ and $F^{|w|}(wx) = x$, if it exsits.

We consider a some order on $\mathcal{A}$, and define an order $wx < w'x$ ($w = a_1 \cdots a_n, w' = b_1 \cdots b_m$) if

- $|w| < |w'|$,
- $|w| = |w'|$, and there exists k such that $a_{k+1} \cdots a_n = b_{k+1} \cdots b_n$ and $a_k < b_k$.

We call a set $\{wx\}$ with the above order a van der Corput sequence generated by the dynamical system (I, F). The famous van der Corput sequece for binary case:

$$0.1, 0.01, 0.11, 0, 001, 0.101, 0.011, 0.111, \ldots$$

corresponds to $d = 1$, $F(x) = 2x \pmod 1$ and $x = \frac{1}{2}$.

2. pseudo random numbers

A sequence $x_1, x_2, \ldots \in I$ is called uniformly distributed if

$$D(N) = \sup_J \Big[\frac{1}{N}\#\{n \leq N\colon x_n \in J\} - |J|\Big]$$

converges to 0 as $N \to \infty$, where supremum is taken over all the intervals in I and $|J|$ is the Lebesgue measure of J.

It is conjectured that any sequence satisfies

$$D(N) \geq O\left(\frac{(\log N)^d}{N}\right).$$

Thus the sequences which satisfies the equality in the above inequality is called of low discrepancy, this means the low discrepancy sequences are the best possible pseudo random numbers. Ninomiya ([9, 10]) showed that the van der Corput sequences generated by β–transformation are of low discrepancy. In 1–dimensional cases, we will extend this result to more general piecewise linear cases, and at the same time, we will construct low discrepancy sequences in higher dimensional cases.

3. Perron–Frobenius Operator

We have constructed pseudo random numbers using dynamical system (I, F). The discrepancy of these sequences are deeply connected with the spectra of the Perron–Frobenius operator P associated with the dynamical system:

$$Pf(x) = \sum_{y \in I, F(y)=x} f(y)\,|J(F)(x)|^{-1},$$

where $J(F)(x)$ is the Jacobian of F at x. In the following we assume that $|J(F)| \equiv \beta$ and $\beta > 1$. In terms of the symbolic dynamics, we can express P by

$$Pf(x) = \sum_{a \in \mathcal{A}} f(ax)\beta^{-1}.$$

The spectra of the Perron–Frobenius operator determine the ergodic properties of the dynamical system:

- 1 is the eigenvalue of the Perron–Frobenius operator, and we can choose a base of the eigenspace by density functions of the invariant measures of the dynamical systems.
- Assume that 1 is the simple eigenvalue, that is, there exists unique invariant probability measure μ. If there exists no eigenvalue modulus 1 except 1, then the dynamical system is mixing.

When we restrict the domain of P to a suitable space (in 1–dimensional cases, BV, the set of functions with bounded

variations), as the first greatest eigenvalue determines the invariant measure, the second greatest eigenvalue in modulus determines the speed of convergence to equilibrium:

$$\int f(x)\, g(F^n(x))\, d\mu \to \int f(x)\, d\mu \int g(x)\, d\mu.$$

4. Renewal equation

In this section, we consider the case of 1–dimensional dynamical systems ($d = 1$), and the partition $\{\langle a\rangle\}_{a\in\mathcal{A}}$ is a partition of $I = [0,1]$ by intervals. We call $\inf\langle a\rangle$ and $\sup\langle a\rangle$ endpoints of $\{\langle a\rangle\}_{a\in\mathcal{A}}$. A point $\inf\langle a\rangle$ is called Markov if $\lim_{x\downarrow\inf\langle a\rangle} F(x)$ also belongs to the set of endpoints, and a point $\sup\langle a\rangle$ is called Markov if $\lim_{x\uparrow\sup\langle a\rangle} F(x)$ also belongs to the set of endpoints. If there exists a partition such that all the endpoints are Markov, then we call F Markov.

Theorem 1 *Assume that there exists no eigenvalues $|z| > \beta^{-1}$ except 1. Let k be the number of non–Markov endpoints, then*

$$D(N) = O\left(\frac{(\log N)^{k+1}}{N}\right).$$

This says the pseudo random numbers can be of low discrepancy only if F is Markov.

5. Renewal Equations

To prove the above theorem, we use renewal equations. To show the outline of the proof, we consider the case of the β–transformation $F(x) = \beta x \pmod 1$, and β equals the golden number $\frac{1+\sqrt{5}}{2}$.

Let $\mathcal{A} = \{a, b\}$ and $\langle a\rangle = [0,\beta^{-1})$, $\langle b\rangle = [\beta^{-1}, 1]$. We define for c either a or b

$$\begin{aligned} s^{\langle c\rangle}(z,x) &= \sum_{n=0}^{\infty} z^n P^n 1_{\langle c\rangle}(x) \\ &= (I - zP)^{-1} 1_{\langle c\rangle}(x). \end{aligned}$$

This suggest that the singularities of $s^{(c)}(z,x)$ equal the reciprocals of the eigenvalues of P.

Now we construct a renewal equation. Note that $F(\langle a\rangle) = I$. Then

$$\begin{aligned} s^{\langle a\rangle}(z,x) &= 1_{\langle a\rangle}(x) + \sum_{n=1}^{\infty} z^n P^{n-1}(P 1_{\langle a\rangle}(x)) \\ &= 1_{\langle a\rangle}(x) + \sum_{n=1}^{\infty} z^n P^{n-1}\Big(\sum_{y\in I, F(y)=\cdot} 1_{\langle a\rangle}(y)\beta^{-1}\Big)(x) \\ &= 1_{\langle a\rangle}(x) + z\beta^{-1}\sum_{n=0}^{\infty} z^n P^n 1_I(x) \\ &= 1_{\langle a\rangle}(x) + z\beta^{-1}\sum_{n=0}^{\infty} z^n P^n (1_{\langle a\rangle}(\cdot) + 1_{\langle b\rangle}(\cdot))(x) \\ &= 1_{\langle a\rangle}(x) + z\beta^{-1}(s^{\langle a\rangle}(z,x) + s^{(b)}(z,x)). \end{aligned}$$

On the other hand, as $F(\langle b\rangle) = \langle a\rangle$, we get

$$s^{\langle b\rangle}(z,x) = 1_{\langle b\rangle}(x) + z\beta^{-1} s^{\langle a\rangle}(z,x).$$

Thus we can express them into the following form:

$$\begin{pmatrix} s^{(a)}(z,x) \\ s^{\langle b\rangle}(z,x) \end{pmatrix} = \begin{pmatrix} 1_{\langle a\rangle}(x) \\ 1_{\langle b\rangle}(x) \end{pmatrix} + \begin{pmatrix} z\beta^{-1} & z\beta^{-1} \\ z\beta^{-1} & 0 \end{pmatrix} \begin{pmatrix} s^{(a)}(z,x) \\ s^{\langle b\rangle}(z,x) \end{pmatrix}.$$

This is a renewal equation for one of the simplest cases. We denote

$$\Phi(z) = \begin{pmatrix} z\beta^{-1} & z\beta^{-1} \\ z\beta^{-1} & 0 \end{pmatrix},$$

and call it the Fredholm matrix. We get

$$\begin{pmatrix} s^{(a)}(z,x) \\ s^{\langle b\rangle}(z,x) \end{pmatrix} = (I - \Phi(z))^{-1} \begin{pmatrix} 1_{\langle a\rangle}(x) \\ 1_{\langle b\rangle}(x) \end{pmatrix}.$$

This suggests that the solutions of $\det(I - \Phi(z)) = 0$ are the reciprocals of the eigenvalues of the Perron–Frobenius operator P. Moreover, we can prove $\det(I - \Phi(z))$ equals the dynamical zeta function

$$\zeta(z) = \exp\left[\sum_{n=1}^{\infty} \frac{z^n}{n} \sum_{p:\, F^n(p)=p} |F^{n\prime}(p)|^{-1}\right].$$

Thus this suggests that the singularities of the dynamical zeta function are also the reciprocals of the eigenvalues of the Perron–Frobenius operator P.

Actually, we can prove the above conjectures are true when we restrict P to BV. We can extend the results to non–Markov transformations. See for detail [3, 4]. Moreover, we can extend the results to higher dimensional cases([7]).

6. Discrepancies

We apply the results of the former section to calculate the discrepancy of the van der Corput sequences. For an interval $J \subset I$, then

$$\#\{wx \in J : |w| = n\} = \sum_{|w|=n} 1_J(wx) = \beta^n P^n 1_J(x).$$

Thus for a word u such that $F^{|u|}(x) = I$

$$\begin{aligned} \sum_{n=0}^{\infty} z^n \#\{wx \in \langle u\rangle : |w| = n\} &= \sum_{n=0}^{\infty} z^n \sum_{|w|=n} 1_{\langle u\rangle}(wx) \\ &= \sum_{n=0}^{\infty} z^n \beta^n P^n 1_{\langle u\rangle}(x) = \sum_{n=0}^{|u|-1} z^n 1_{F^n(\langle u\rangle)}(x) + z^{|u|} s^I(\beta z, x). \end{aligned}$$

On the other hand, if N equals the number of words for which the length is less than or equal to n, then

$$\frac{1}{N}\sum_{k=0}^{n} \#\{wx \in J : |w| = k\} = \frac{1}{N}\sum_{k=0}^{n} \beta^k P^k 1_J(x).$$

Thus we can calculate it using the k–th coefficient of $s^J(z,x)$ ($k \le n$), and we get the proof of Theorem 1. See for detail [5, 6], and the computer simulation of this pseudo random numbers, see [1].

7. Higher Dimensional cases

We can also construct a renewal equation for $d \geq 2$. However, the essential spectral radius of the Perron–Frobenius operator is usually greater than β^{-1}. Thus it is very difficult to construct pseudo random numbers of low discrepancy. We will construct it using irreducible polynomials.

We consider a d–dimensional irreducible polynomial $p(\beta)$ on $\mathbb{F}_2$. We express by $\hat{\mathcal{A}} = [1, \beta, \ldots, \beta^{d-1}]$ the additive group generated by $\{1, \beta, \ldots, \beta^{d-1}\}$.

We identify β^k $(0 \leq k \leq d-1)$ as $\begin{pmatrix} \alpha_0^k \\ \vdots \\ \alpha_{d-1}^k \end{pmatrix} \in \mathcal{A}$ such that $\alpha_k^k = 1$ and $\alpha_i^k = 0$ $(i \neq k)$. Thus for $x \in [0,1]^d$ with its binary expansion $0.\alpha_1\alpha_2\cdots$ $(\alpha_k \in \mathcal{A})$, we can identify it as a sequence of $\tilde{\mathcal{A}}$. Instead of constructing $F\colon [0,1]^d \to [0,1]^d$, we will construct $\hat{F}\colon \tilde{\mathcal{A}}^{\mathbb{N}} \to \tilde{\mathcal{A}}^{\mathbb{N}}$.

Let $A_i = \begin{pmatrix} 1 \\ \beta^{2^{i-1}} \\ \beta^{2\cdot 2^{i-1}} \\ \vdots \\ \beta^{(d-1)2^{i-1}} \end{pmatrix}$ $(1 \leq i \leq d)$. and consider a matrix $(A_1, A_2 \ldots, A_d)$. Note that this matrix has inverse on $\mathbb{F}_2$. We denote its inverse matrix by $\begin{pmatrix} X_1 \\ \vdots \\ X_d \end{pmatrix}$, where X_i is a d–dimensional row vector.

Example 1 *For $d = 3$ and $p(\beta) = 1 + \beta + \beta^3$,*

$$(A_1, A_2, A_3) = \begin{pmatrix} 1 & 1 & 1 \\ \beta & \beta^2 & \beta^4 \\ \beta^2 & \beta^4 & \beta^8 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ \beta & \beta^2 & \beta+\beta^2 \\ \beta^2 & \beta+\beta^2 & \beta \end{pmatrix},$$

and

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} 1 & \beta^2 & \beta \\ 1 & \beta^4 & \beta^2 \\ 1 & \beta & \beta^4 \end{pmatrix} = \begin{pmatrix} 1 & \beta^2 & \beta \\ 1 & \beta+\beta^2 & \beta^2 \\ 1 & \beta & \beta+\beta^2 \end{pmatrix}.$$

We will define infinite dimensional matrices $U = (a_{ij})_{i,j\geq 1}$ and $V = (x_{ij})_{i,j\geq 1}$, where a_{ij} is a d–dimensional column vector of $\mathcal{A}$ and x_{ij} is a d–dimensional row vector of $\mathcal{A}$. Note that in U, 0 means the d–dimensional zero column vector, and in V, 0 means the d–dimensional zero row vector. Let us define rule A by

$$\tilde{a}_{ij} = \begin{cases} \tilde{a}_{i-1,j-1} & j = 1 \pmod d, \\ \tilde{a}_{i-1,j-1} + \tilde{a}_{i.j-1} \pmod 2 & \text{otherwise.} \end{cases}$$

with initial condition $\tilde{a}_{11} = 1$ and $\tilde{a}(0,i) = 0$, and we define a matrix U by

$$a_{ij} = \begin{cases} A_k & \text{if } \tilde{a}_{ij} = 1, \text{and } j = k \pmod d, \\ 0 & \text{if } \tilde{a}_{ij} = 0. \end{cases}$$

Let $\tilde{x}_{ij}$ also satisfy rule A with initial condition $\tilde{x}_{ij} = 1$ if $\lceil \frac{i-1}{d} \rceil = j$ and $\tilde{x}_{ij} = 0$ if $\lceil \frac{i-1}{d} \rceil < j$. We define a matrix V by

$$x_{ij} = \begin{cases} X_k & \text{if } \tilde{x}_{ij} = 1, \text{and } i = k \pmod d, \\ 0 & \text{if } \tilde{x}_{ij} = 0. \end{cases}$$

Example 2 *For $d = 3$, U equals*

$$U = \begin{pmatrix} A_1 & A_2 & A_3 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & A_2 & 0 & A_1 & A_2 & A_3 & 0 & 0 & 0 & \cdots \\ 0 & 0 & A_3 & 0 & A_2 & 0 & A_1 & A_2 & A_3 & \cdots \\ 0 & 0 & 0 & A_1 & A_2 & 0 & 0 & A_2 & 0 & \cdots \\ 0 & 0 & 0 & 0 & A_2 & 0 & 0 & 0 & A_3 & \cdots \\ 0 & 0 & 0 & 0 & 0 & A_3 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

and V equals

$$V = \begin{pmatrix} X_1 & 0 & 0 & 0 & 0 & \cdots \\ X_2 & 0 & 0 & 0 & 0 & \cdots \\ X_3 & 0 & 0 & 0 & 0 & \cdots \\ 0 & X_1 & 0 & 0 & 0 & \cdots \\ X_2 & X_2 & 0 & 0 & 0 & \cdots \\ 0 & X_3 & 0 & 0 & 0 & \cdots \\ 0 & 0 & X_1 & 0 & 0 & \cdots \\ X_2 & X_2 & X_2 & 0 & 0 & \cdots \\ X_3 & 0 & X_3 & 0 & 0 & \cdots \\ 0 & X_1 & 0 & X_1 & 0 & \cdots \\ 0 & 0 & X_2 & X_2 & 0 & \cdots \\ 0 & 0 & 0 & X_3 & 0 & \cdots \\ 0 & 0 & 0 & 0 & X_1 & \cdots \\ X_2 & X_2 & X_2 & X_2 & X_2 & \cdots \\ X_3 & 0 & X_3 & 0 & X_3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

These form Sierpinskii gaskets.

We define a transformation $\hat{F}$ by

$$V\hat{F}U = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

that is, $V\hat{F}U$ is the shift.

Then for a rectangular J which is a union of intervals corresponding to words such that its length of edges $l_1, \ldots, l_d$ satisfies $l_1 \times l_2 \cdots \times l_d = 2^{-kd}$, we can show $F^k(J) = I$. From this fact, we can prove that the essential spectral radius of the Perron–Frobenius operator equals 2^{-d} and there exists no eigenvalue except 1 in $|z| > 2^{-d}$, thus the van der Corput sequence generated by this transformation is of low discrepancy. See for detail [2, 8].

References

[1] Yuko Ichikawa and Makoto Mori, "Discrepancy of van der Corput sequences generated by piecewise lin-

ear transformations", *Monte Carlo methods and Applications* vol.10, pp.107-116, 2004.

[2] Masaki Mori and Makoto Mori, "New Construction of two dimensional Low Discrepancy Sequences", *Proceedings of The Institute of Natural Sciences, Nihon University*. vol.47, pp. 449–462, 2012.

[3] Makoto Mori, "Fredholm determinant for piecewise linear transformations", *Osaka J. Math.*, vol.27, pp. 81-116, 1990.

[4] Makoto Mori, "Fredholm determinant for piecewise monotonic transformations", *Osaka J. Math.*, vol.29, pp. 497-529, 1992.

[5] Makoto Mori, "Low discrepancy sequences generated by piecewise linear Maps", *Monte Carlo methods and Applications*, vol.4, pp. 141-162, 1998.

[6] Makoto Mori, "Discrepancy of sequences generated by piecewise monotone Maps", *Monte Carlo methods and Applications*, vol.5, pp.55-68, 1999.

[7] Makoto Mori, "Fredholm determinant for higher dimensional piecewise linear transformations", *Japanese J. Math.*, vol.25, pp. 317–342, 1999.

[8] Makoto Mori, "Dynamical system generated by algebraic method and low discrepancy sequences", *Monte Carlo Methods and Applications*, vol.18, pp. 327-351, 2012.

[9] S. Ninomiya, "Constructing a new class of low-discrepancy sequences by using the β-adic transformation", *Math. Comput. Simul.*, vol.47, pp. 405-420, 1998.

[10] S. Ninomiya, "On the discrepancy of the β-adic van der Corput sequence", *J. Math. Sci. Univ. Tokyo*, vol.5, pp. 345-366, 1998.