Numération : mathématiques et informatique

RENCONTRE ORGANISÉE PAR :
Boris Adamczewski, Anne Siegel and Wolfgang Steiner

23-27 mars 2009

Makoto Mori

On random numbers generated by Dynamical systems

Vol. 1, n° 1 (2009), p. 49-53.

<http://acirm.cedram.org/item?id=ACIRM_2009__1_1_49_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) FRANCE

Actes des rencontres du C.I.R.M.
Vol. **1** n^o 1 (2009) 49-53

On random numbers generated by Dynamical systems

Makoto Mori

1. Summary

Let us consider a dynamical system (I, F), where $I = [0,1]^d$. We denote it as symbolic dynamics on a finite set $\mathcal{A}$.

- $\{\langle a \rangle\}_{a\in\mathcal{A}}$ is a partition of I,
- $F_a = F|_{\langle a \rangle}$ is 1 to 1.

Then, $x \in I$ corresponds to a sequence $a_1^x a_2^x \cdots \in \mathcal{A}^{\mathbb{N}}$ by

$$F^{n-1}(x) \in \langle a_n^x \rangle.$$

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

- $|w| = n$,
- $\langle w \rangle = \bigcap_{i=1}^n F^{-i+1}(\langle a_i \rangle)$,
- if $\langle w \rangle \neq \emptyset$, then w is called admissible,
- $wx \in \langle w \rangle$ and $F^{|w|}(wx) = x$, if it exists,
- $\mathcal{W}$ is the set of admissible words and the empty word ϵ, where we define $\langle \epsilon \rangle = I$.

The main tool to study the ergodic properties of the dynamical system is the Perron–Frobenius operator, which is defined for $f \in L^1$ by

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

This satisfies for $g \in L^\infty$

$$\int f(x)\, g(F^n(x))\, dx = \int P^n f(x)\, g(x)\, dx.$$

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

- If $P\rho = \rho$, $\rho \geq 0$ and $\int \rho\, dx = 1$, then ρ is the density of an invariant probability measure μ.
- If the eigenvalue 1 is simple, then the dynamical system is ergodic.
- If there exists no eigenvalue on the unit circle except 1, then the dynamical system is mixing.

If the dynamical system (I, μ, F) is mixing, then for $f \in L^1$ and $g \in L^\infty$

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

We call the speed of convergence by decay rate of correlation. This is determined by the second greatest eigenvalue of P in modulus.

In this article, we consider only the case $|F'(x)| \equiv \beta > 1$, then

$$P^n f(x) = \sum_{|w|=n} f(wx)\beta^{-n}.$$

Text presented during the meeting "Numeration: mathematics and computer science" organized by Boris Adamczewski, Anne Siegel and Wolfgang Steiner. 23-27 mars 2009, C.I.R.M. (Luminy).

The essential spectrum radius of P equals 1. So, in 1–dimensional cases, we restrict P to the set of functions with bounded variation. Then the essential spectrum radius equals $\frac{1}{\beta} = e^{-\xi}$, where

$$\xi = \liminf_{n\to\infty} \frac{1}{n} \inf_{x\in[0,1]} \log |F^{n\prime}(x)|.$$

Now we consider higher dimensional cases. Let $\mathcal{B}$ be the set of functions for which there exists a partition $f = \sum_{w\in\mathcal{W}} C_w 1_{\langle w\rangle}$ such that for any $0 < r < 1$

$$||f||_r = \inf \sum_{m=0}^{\infty} r^m \sum_{|w|=m} |C_w| < \infty,$$

where inf is taken over all decompositions of f. Then, $\mathcal{B}$ becomes a locally convex space with semi norms $||\cdot||_r$ $(0 < r < 1)$. This is the slight extention of the set of functions with bounded variations in 1–dimensional cases, because we can choose a decomposition such that $\sum_{|w|=m} |C_w|$ is less than or equal to the total variation of f. Thus all the functions with bounded variation belongs to $\mathcal{B}$. We can show that when we restrict the Perron–Frobenius operator to $\mathcal{B}$ the decay rate of correlation is the second greatest eigenvalue of it.

We can determine the spectra of the Perron–Frobenius operator resitricted to $\mathcal{B}$ by eigenvalues of a finite dimensional matrix which we call a Fredholm matrix([2, 3, 6]).

For higher dimensional cases, we can also determine the Lyapunov index by

$$\xi = \liminf_{n\to\infty} \frac{1}{n} \inf_{x\in[0,1]} \log |\det F^{n\prime}(x)|,$$

where $|\det F^{n\prime}(x)|$ is the Jacobian of F^n. However, the essential spectrum radius of the Perron–Frobenius operator restricted to $\mathcal{B}$ is in general greater than $e^{-\xi}$. For example, for

$$F(x) = 2x \pmod 1,$$

the essential spectrum radius equals $2^{1-d} > 2^{-d} = e^{-\xi}$.

Thus, we want to study the mechanism that the essential spectrum radius coincide with $e^{-\xi}$.

2. Low Discrepancy Sequence

For a sequence $x_1, x_2, \ldots \in [0,1]^d$, there exists a constant C such that

$$D_N \geq C \frac{(\log N)^d}{N}$$

holds when $d = 1, 2$ (W.Schmidt), and even for $d \geq 3$ it is conjectured (Roth's conjecture). Here D_N is the discrepancy defined by

$$D_N = \sup_J \left| \frac{\#\{x_i \in J : i \leq N\}}{N} - |J| \right|,$$

where $\sup_J$ is taken over all intervals and $|J|$ is the Lebesgue measure of J.

If $D_N = O(\frac{(\log N)^d}{N})$, we call a sequence $x_1, x_2, \ldots \in [0,1]^d$ a pseudo random sequence of low discrepancy. These sequences are useful to calculate integrations numerically.

One of the most famous example of low discrepancy sequences is the van der Corput sequence. We will construct it using a dynamical system.

We will define an order on a set of words as follows:

- $w < w'$ if $|w| < |w'|$,
- for $w = a_1 \cdots a_n$ and $w' = b_1 \cdots b_n$, $w < w'$ if $a_k = b_k$ for $k \geq m+1$ and $a_m < b_m$.

Choose any $x \in I$, then our van der Corput sequence is the set of $\{wx\}$ arranged in the above order.

For $F(x) = 2x \pmod 1$, the order of words are

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots.$$

Thus our van der Corput sequence is

$$x, 0x, 1x, 00x, 10x, 01x, 11x, 000x, 100x, \ldots.$$

Original van der Corput sequence is determined by the sequence of integers $1, 10, 11, 100, 101, 110, 111, 10000$:

0.1	0.01	0.11	0.001	0.101	0.011	0.111	0.0001	...
$1x$	$01x$	$11x$	$001x$	$101x$	$011x$	$111x$	$0001x$	....

Then they equals when we take $x = \frac{1}{2}$.

Theorem 1 ([4])**.** *For a piecewise linear Markov and transformation F with same slope $|F'(x)| \equiv \beta > 1$ on $[0,1]$, the van der Corput sequence is of low discrepancy if and only if there exists no eigenvalue of P restricted to $\mathcal{B}$ except the simple eigenvalue 1 in $|z| > 1/\beta = e^{-\xi}$.*

For 1–dimensional cases, we can also show the similar results when F is not Markov ([5]).

3. 2 dimensional cases

Now we will construct two dimensional low discrepancy sequences. For this purpose, we need to construct transformations for which the essential spectrum radius of P restricted to $\mathcal{B}$ equals $e^{-\xi}$. Let

$$\mathcal{A} = \{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\}.$$

We need to construct a transformation satisfying the following conditions. For a word $w = i_1 \cdots i_n$ $(i_k \in \mathcal{A})$, $F^n(\langle w \rangle) = I$.

Moreover, for any rectangle R with length $2^{-n-k} \times 2^{-n+k}$ $(0 \le k \le n)$ which is 2^{2k} union of words with length $n+k$, $F^n(R) = I$. Then the essential spectrum radius equals $\frac{1}{4}$ and there exists no unessential eigenvalues except 1. Thus, this generates low discrepancy sequences.

3.1. **One example** ([7, 8])**.**

Let $s_0 = 00\cdots$.

$$\begin{aligned} s_1 &= \ 1\ 0\ 1\ 0 \cdots \\ \theta s_1 &= \ 0\ 1\ 0 \cdots \\ \theta^2 s_1 &= 1\ 0\ 0 \cdots \\ \cdots &= \ \cdots \end{aligned}$$

Here s_1 is determined such that the first n symbols of $s_1, \theta s_1, \ldots, \theta^{n-1}s_1$ generate all the words with length n. We define

$$F\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\theta x\\ \theta y\end{pmatrix} + \begin{pmatrix}s_{y_1}\\ s_{x_1}\end{pmatrix},$$

where we identify $x \in [0,1]$ and its binary expansion $x_1x_2\cdots$. Then for any interval $J = [k2^{-N-n}, (k+1)2^{-N-n}) \times [l2^{-N+n}, (l+1)2^{-N+n})$, $F^N(J) = I$ without overlap.

From this fact, we can prove the van der Corput sequence generated by this transformation is of low discrepancy. Unfortunately, this method can only extend until 3–dimensional cases.

3.2. **Another example.**

We will define a substitution

$$F(abc) = d, \qquad a, b, c, d \in \mathcal{A}.$$

From this substitution, we can define a transformation

$$F(a_1a_2\cdots) = b_1b_2\cdots$$

by

$$F(a_ia_{i+1}a_{i+2}) = b_{i+1} \quad (i \ge 1),$$

and the substitution $F(a_1a_2) = b_1$ is defined afterwards.

We introduce a commutative group of actions on $\mathcal{A}$

$$\{S, H, V, C\}.$$

where

$$S\begin{pmatrix}i\\j\end{pmatrix} = \begin{pmatrix}i\\j\end{pmatrix}, \quad H\begin{pmatrix}i\\j\end{pmatrix} = \begin{pmatrix}i'\\j\end{pmatrix},$$
$$V\begin{pmatrix}i\\j\end{pmatrix} = \begin{pmatrix}i\\j'\end{pmatrix}, \quad C\begin{pmatrix}i\\j\end{pmatrix} = \begin{pmatrix}i'\\j'\end{pmatrix},$$

where $i' = i+1 \pmod 1$ and $j' = j+1 \pmod 1$. Then

$$S+S = H+H = V+V = C+C = S$$
$$H+V = C,\ H+C = V,\ V+C = H.$$

We define a substitution F which satisfies

$$F(((A+A')a)((B+B')b)((C+C')c)) = F((Aa)(Bb)(Cc)) + F((A'a)(B'b)(C'c)).$$

Now instead of a substitution on $\mathcal{A}$, we will determine a substitution on $\{S, H, V, C\}$.

We call a set of words

$$\{SS, HC, CV, VH\}$$

a family and denote it by $\mathcal{F}_S$, and define

$$\mathcal{F}_A = \mathcal{F}_S + AA, \quad (A \in \mathcal{A}),$$

that is,

$\mathcal{F}_S$	SS	HC	VH	CV
$\mathcal{F}_C$	SH	HV	VS	CC
$\mathcal{F}_V$	SC	HS	VV	CH
$\mathcal{F}_H$	SV	HH	VC	CS

Note that $\mathcal{F}_S$ is a group, and chosen one from each row and column. There exists another candidate $\{SS, HV, VC, CH\}$. We will explain our idea using $\mathcal{F}_S$ in this article.

We call

$$\{a_A b_A : A \in \mathcal{A}\} \subset \mathcal{A}^2$$

a complete pair if $a_A b_A \in \mathcal{F}_A$. Then $\{SS, SH.HS.HH\}$ and $\{SS, SV.VS, VV\}$ are complete pairs.

We will construct $F \colon \mathcal{A}^3 \to \mathcal{A}$. We find a group $\mathcal{G}_S$ and define

	S	H	V	C
$\mathcal{G}_S$	SSS	CVH	HCV	VHC
	HHS	VCH	SSV	CSC
	VVS	HSH	CHV	SCC
	CCS	SHH	VSV	HVC
$\mathcal{G}_H$	CVS	SSH	VHV	HCC
	VCS	HHH	CSV	SVC
	HSS	VVH	SCV	CHC
	SHS	CCH	HVV	VSC
$\mathcal{G}_V$	HCS	VHH	SSV	CVC
	SVS	CSH	HHV	VCC
	CHS	SCH	VVV	HSC
	VSS	HVH	CCV	SHC
$\mathcal{G}_C$	VHS	HCH	CVV	SSC
	CSS	SVH	VCV	HHC
	SCS	CHH	HSV	VVC
	HVS	VSH	SHV	CCC

Then there exists three cases which satisfy the following Lemma 1. One of them are the following.

$$F(abc) = \begin{cases} S & \text{if } abc \in \mathcal{G}_S, \\ H & \text{if } abc \in \mathcal{G}_V, \\ V & \text{if } abc \in \mathcal{G}_H, \\ C & \text{if } abc \in \mathcal{G}_C. \end{cases}$$

We also define for the first two symbols:

$$F(a_1a_2) = \begin{cases} S & \text{if } a_1a_2 \in \mathcal{F}_S, \\ H & \text{if } a_1a_2 \in \mathcal{F}_H, \\ V & \text{if } a_1a_2 \in \mathcal{F}_C, \\ C & \text{if } a_1a_2 \in \mathcal{F}_V. \end{cases}$$

Lemma 1. (1) *For fixed $a, b \in \mathcal{A}$,*

$$\text{the last two symbols of } \{F(abcd)\colon cd \in \mathcal{F}_A\} = \mathcal{F}_B \qquad \exists B \in \mathcal{A},$$

and for differnt $A \in \mathcal{A}$ B is different.

(2) *For a fixed $f \in \mathcal{A}$, there exists $B \in \mathcal{A}$ such that for any $de \in \mathcal{F}_A$*

$$\text{the last two symbols of } \{F(abcde)\colon F(abc) = f\} = \mathcal{F}_B.$$

Now, we call a set $\{a_1 \cdots a_n\}$ of type $(n, 0)$, and for a complete set $\mathcal{C}$ $\{a_1 \cdots a_n w\colon w \in \mathcal{C}\}$ of type $(n, 1)$. The we define inductively

$$\bigcup_{i_1,\dots,i_k=1}^{4} \{a_1 \cdots a_n w_{i_1} w_{i_1 i_2} w_{i_1 i_2 i_3} \cdots w_{i_1 \cdots i_k}\}$$

is of type (n, k) if

$$\bigcup_{i_1,\dots,i_{k-1}=1}^{4} \{a_1 \cdots a_n w_{i_1} w_{i_1 i_2} w_{i_1 i_2 i_3} \cdots w_{i_1 \cdots i_{k-1}}\}$$

is of type $(n, k-1)$ and for each $i_1, \dots, i_{k-1}$

$$\bigcup_{i_k=1}^{4} \{a_1 \cdots a_n w_{i_1} w_{i_1 i_2} w_{i_1 i_2 i_3} \cdots w_{i_1 \cdots i_k}\}$$

is of type $(n + 2(k-1), 1)$. Moreover, we call a set A of words with length $n + 2k$ of type $(\mathcal{A}^n, k)$ if

$$A = \bigcup_{a_1,\dots,a_n \in \mathcal{A}} A_k(a_1, \dots, a_n),$$

where $A_k(a_1, \dots, a_n)$ is a set of words of type (n, k).

Then by Lemma 1, we get

Lemma 2. (1) *For a set A of words of type (n, k), $F(A)$ is of type $(n-1, k)$.*
(2) *For a set A of words of type $(\mathcal{A}^n, k)$, $F(A)$ is of type $(\mathcal{A}^{n+1}, k-1)$.*

By Lemma 2, we can prove:

Theorem 2. *The van der Corput sequence generaed by this transformation F is of low discrepancy.*

We expect by this method we can construct higher dimensional low discrepancy sequences.

References

[1] Y. Ichikawa and M. Mori, *Discrepancy of van der Corput sequences generated by piecewise linear transformations*, Monte Carlo methods and Applications **10** No. 2(2004) 107-116.

[2] M. Mori, *Fredholm determinant for piecewise linear transformations*, Osaka J. Math. **27**(1990) 81-116.

[3] M. Mori, *Fredholm determinant for piecewise monotonic transformations*, Osaka J. Math. **29**(1992) 497-529.

[4] M. Mori, *Low discrepancy sequences generated by piecewise linear Maps*, Monte Carlo methods and Applications **4** No. 2(1998) 141-162.

[5] M. Mori, *Discrepancy of sequences generated by piecewise monotone Maps*, Monte Carlo methods and Applications **5** No. 1(1999) 55-68.

[6] M. Mori, *Fredholm determinant for higher dimensional piecewise linear transformations*, Japanese J. Math. **25** No.2(1999) 317–342.

[7] M. Mori, *Construction of two dimensional low discrepancy sequences*, Monte Carlo methods and Applications **8** No.2(2002) 159-170.

[8] M. Mori, *Construction of 3 dimensional low discrepancy sequences*, Monte Carlo methods and Applications **11** No.2(2005) 163-174.

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

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

Dept. Math., College of Humanities and Sciences,, Nihon University