2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

Discretized Markov Transformations
– An Example of Ultradiscrete Dynamical Systems –

Hiroshi Fujisaki

Graduate School of Natural Science and Technology,
Kanazawa University,
40-20 Kodatsuno 2 chome, Kanazawa,
Ishikawa, 920-8667 Japan
Email: fujisaki@t.kanazawa-u.ac.jp.

Abstract—We define discretized Markov transformations and find an algorithm to give the number of maximal-period sequences based on discretized Markov transformations. In this report, we focus on discretized dyadic transformations and define a number-theoretic function related to the numbers of maximal-period sequences based on the discretized dyadic transformations. We also introduce the entropy of the maximal-period sequences based on discretized dyadic transformations.

1. Introduction

It's been an age since Ulam and von Neumann pointed out that, given an initial value, the sequence of iterating one-dimensional ergodic transformation, for instance a logistic transformation: $T(x) = 4x(1-x)$, is a good candidate for a pseudo-random numbers [1]. These sequences are intended for Monte Carlo applications. At that time, the availability and the use of computers are restricted.

Things have changed in the past two decades, and the computer age has come. The computers are now very inexpensive and ubiquitous. These situations enable us to propose the sequences of pseudo-random numbers generated by one-dimensional ergodic transformations to be used as spreading sequences in SSMA (spread spectrum multiple access) communication systems (see [2] for instance) and as real-valued keystream in so called chaotic encryption systems. Unfortunately, however, they are not available for practical use.

To begin with, Ulam and von Neumann's idea requires handling real numbers for practice. On the contrary, computers can only deal with floating point numbers. Hence we need ergodic theory for a transformation from a finite set onto itself to understand the behaviour of the iterates of one-dimensional transformations implemented in computers. Unfortunately, no way is known to give a good theoretical model that tells us characteristics of the execution time for floating point numbers [3].

Recently a breakthrough has been made as follows: discretized Bernoulli transformations were considered and their applications to cryptography and SSMA communication systems were proposed [4]-[5]. The discretized ergodic transformation is a permutation of subintervals determined by the transformation. We may say that this is an example of *ultradiscrete* dynamical systems [6]. If we use the discretized ergodic transformations, we need not care for floating point number computation. This is a great advantage of using the discretized ergodic transformations rather than implementing the original ergodic transformations in a computer system.

In [5], maximal-period sequences based on discretized Bernoulli transformations were proposed and their correlational properties were numerically investigated. It is pointed out in [5] that the maximal-period sequences based on discretized dyadic transformation were a generalization of de Bruijn sequences. While the number of de Bruijn sequences are well known [7], the numbers of maximal-period sequences based on several discretized Bernoulli transformations were numerically conjectured in [5].

In this report, we define discretized Markov transformations and give an algorithm to give the number of maximal-period sequences based on discretized Markov transformations. This gives a proof to Tsuneda et al.'s numerical conjecture on the numbers of maximal-period sequences based on discretized Bernoulli transformations. We also define a number-theoretic function relating to the numbers of maximal-period sequences based on discretized dyadic transformations. Finally we discuss the entropy of the maximal-period sequences based on discretized dyadic transformations.

2. Preliminaries

In graph theory, technical terminology does not seem to be unified. Firstly we shall give some definitions of the graph theoretic notions frequently used throughout this study.

A *graph* $G = (\mathcal{V}, \mathcal{E})$ is defined by a finite set $\mathcal{V}$ whose

elements are called *vertices* together with a set $\mathcal{E}$ of two-element subsets of $\mathcal{V}$. The elements of $\mathcal{E}$ are called *edges*. In our definitions, *multiple* edges are allowed. For $e = \{u, v\} \in \mathcal{E}$ $(u, v \in \mathcal{V})$, we say that e is *incident* with u and v. The number of edges incident with v is called the *degree* of a vertex v. A *walk* in a graph G is defined by an alternating sequence of vertices and edges: $v_0 e_1 v_1 \cdots e_n v_n, \quad v_{i-1}, v_n \in \mathcal{V}, \quad e_i = \{v_{i-1}, v_i\} \in \mathcal{E} \quad (i = 1, 2, \cdots, n)$. If $v_0 = v_n$, then the walk is called *closed*. A walk in which all edges are distinct is called a *path*. If a path from u and v exists for every pair of vertices u, v of G, then G is called *connected*.

An *Eulerian circuit* in a graph is a closed path through a graph using every edge once. If a graph G has an Eulerian circuit, then we say that G is an *Eulerian graph*. The following theorem is celebrated for establishing graph theory:

Theorem 1 (Euler [8]) *A graph G is Eulerian if and only if it is connected and every vertex has even degree.*

A *directed graph* $G = (\mathcal{V}, \mathcal{A})$ is defined by a finite set $\mathcal{V}$ together with a set $\mathcal{A}$ of ordered pairs of elements of $\mathcal{V}$. These pairs are called *arcs*. In our definitions, *multiple* arcs and *loops* $\ell = (v, v) \in \mathcal{A}$ $(v \in \mathcal{V})$ are allowed. We denote an arc (u, v) by uv. The arc uv goes from u to v and is *incident* with u and v. We also say that u is *adjacent to* v and v is *adjacent from* u. The *out-degree* of a vertex v denoted by $\mathrm{odeg}(v)$ is the number of vertices adjacent from it, and the *in-degree* of a vertex v denoted by $\mathrm{ideg}(v)$ is the number adjacent to it. A (*directed*) *walk* in a directed graph G is an alternating sequence of vertices and arcs $v_0 a_1 v_1 \cdots a_n v_n, \quad v_{i-1}, v_n \in \mathcal{V}, \quad a_i = v_{i-1} v_i \in \mathcal{A} \quad (i = 1, 2, \cdots, n)$. If $v_0 = v_n$, then a walk is called *closed*. A walk in which all arcs are distinct is called a *path*. A directed graph G is called *strongly connected* if a path from u and v exists for every pair of distinct vertices u, v of G. Every directed graph $G = (\mathcal{V}, \mathcal{A})$ naturally corresponds to an ordinary graph $G_0 = (\mathcal{V}, \mathcal{E})$, where G_0 has an edge incident with u and v if and only if $u \neq v$ and G has an arc from u to v or from v to u; we say that G is *connected* if the corresponding graph G_0 is connected.

Let G be a directed graph with vertices $v_1, v_2, \cdots, v_n$, and with a_{jk} arcs leading from v_j to v_k $(j, k = 1, 2, \cdots, n)$. We write $\sigma_j = \sum_{k=1}^{n} a_{jk} = \mathrm{odeg}(v_j); \quad \tau_k = \sum_{j=1}^{n} a_{jk} = \mathrm{ideg}(v_k)$.

Definition 1 (de Bruijn [7], Harary and Norman [9]) *The arc digraph G^* is a directed graph with $\sum_{j=1}^{n} \sigma_j$ vertices, one for each arc of G; a vertex of G^*, which corresponds to an arc from v_j to v_k in G, will be denoted A_{jk}. G^* has exactly 0 or 1 arcs leading from A_{jk} to $A_{j'k'}$ according as $k \neq j'$ or $k = j'$.*

There may be several vertices of G^* with the same name A_{jk}, but they will be regarded as distinct. G^* has $\sum_{i=1}^{n} \sigma_i \tau_i$ arcs.

3. De Bruijn Sequences

A *binary word* (or *block*) is a finite binary sequence. We denote the length of a word b by $|b|$. A word of length n is called an *n-word*. We denote the set of all n-words over $\{0, 1\}$ by $\{0, 1\}^n$.

A (*binary*) *cycle* of length k is a sequence of k digits $a_1 a_2 \cdots a_k$ taken in a circular order. In the cycle $a_1 a_2 \cdots a_k$, a_1 follows a_k, and $a_2 \cdots a_k a_1, \cdots, a_k a_1 \cdots a_{k-1}$ are all the same cycle as $a_1 a_2 \cdots a_k$.

A (*binary*) *complete cycle* of length 2^n is a cycle of binary 2^n-word, such that the 2^n possible ordered sets of binary n-word of that cycle are all different. Any binary n-word occurs exactly once in the complete cycle.

Because of the following theorem, the complete cycles are sometimes called de Bruijn sequences.

Theorem 2 (de Bruijn [7], Flye Sainte-Marie [10]) *For each positive integer n, there are exactly $2^{2^{n-1}-n}$ complete cycles of length 2^n.*

In fact this theorem is a corollary of

Theorem 3 (de Bruijn [7]) *Let G be a directed graph with m vertices such that* $\mathrm{odeg}(v) = \mathrm{ideg}(v) = 2$ *for every vertex v. If G has exactly M complete cycles, then its arc digraph G^* has exactly $2^{m-1}M$ complete cycles.*

This theorem was proved using combinatorial methods.

Theorem 2 enables us to determine the number of k-ary complete cycles:

Remark 1 *For each positive integer n, there are exactly $\{(k-1)!\}^{k^{n-1}} k^{k^{n-1}-n}$ complete cycles of length k^n.*

4. Discretized Dyadic Transformations

Let $T : [0, 1] \to [0, 1]$. Let $\mathcal{P}$ be a partition of $[0, 1]$ given by the point $0 = a_0 < a_1 < \cdots < a_{\#\mathcal{P}} = 1$. For $i = 1, \cdots, \#\mathcal{P}$, let $I_i = (a_{i-1}, a_i)$ and denote the restriction of T to I_i by $T|_{I_i}$. If $T|_{I_i}$ is a homeomorphism from I_i onto some connected union of intervals of $\mathcal{P}$, then T is said to be *Markov*. The partition $\mathcal{P} = \{I_i\}_{i=1}^{\#\mathcal{P}}$ is referred to as a *Markov partition with respect to T*.

As the simplest example of discretized Markov transformations, we focus on discretized dyadic transformations. Let $T : [0, 1] \to [0, 1]$ be the dyadic transformation: $T(x) = 2x \pmod 1, \quad x \in [0, 1]$.

Let $\mathcal{P}_m$ be a partition of $[0,1]$ given by the point

$$0 < 1/2m < 2/2m < \cdots < 1 - 1/2m < 1.$$

For $i = 1, \cdots, 2m$, let $I_i = ((i-1)/2m, i/2m)$. Thus the partition $\mathcal{P}_m = \{I_i\}_{i=1}^{2m}$ is a Markov partition with respect to T.

Definition 2 *For each m, the discretized dyadic transformation $\widehat{T}$ is defined by a permutation $\widehat{T} : \mathcal{P}_m \to \mathcal{P}_m$ with $\widehat{T}(I_i) \subset T|_{I_i}(I_i)$ for $i = 1, \cdots, 2m$.*
We denote the set of all discretized dyadic transformations by $\mathcal{T}_m$.

Example 1 *We give an example of discretized dyadic transformations (m=6):*

$$\widehat{T} = \begin{pmatrix} I_1 & I_2 & I_3 & I_4 & I_5 & I_6 & I_7 & I_8 & I_9 & I_{10} \\ I_2 & I_3 & I_5 & I_7 & I_9 & I_{12} & I_1 & I_4 & I_6 & I_8 \end{pmatrix} \begin{pmatrix} I_{11} & I_{12} \\ I_{10} & I_{11} \end{pmatrix}.$$

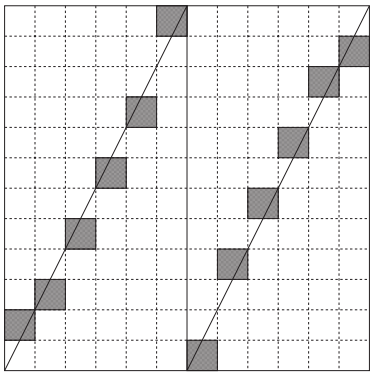

Figure 1: An Example of Discretized Dyadic Transformations (m=6)

This permutation can be represented by binary 6*-word* 100001 *corresponding the relation between I_i and $\widehat{T}(I_i)$ for $i = 1, 2, \cdots, 6$.*

Let us consider a code of discretized dyadic transformations. Let $\widehat{T} \in \mathcal{T}_m$. Note that $\#\mathcal{T}_m = 2^m$. We define a bijection $\phi : \mathcal{T}_m \to \{0,1\}^m$ by $\phi(\widehat{T}) = a_1 a_2 \cdots a_m$ where

$$a_i = \begin{cases} 1 & \text{for } \widehat{T}(I_i) = I_{2i}, \\ 0 & \text{for } \widehat{T}(I_i) = I_{2i-1}, \end{cases} \qquad i = 1, 2, \cdots, m. \tag{1}$$

For a given binary m-word a, we simply write $\phi^{-1}(a) = \widehat{T}_a$.

Let $\widehat{T} \in \mathcal{T}_m$. Consider a sequence of subintervals from $\mathcal{P}_m$: $(\widehat{T}^n(I_1))_{n=0}^{\infty}$ where $\widehat{T}^0(I_1) = I_1$ and $\widehat{T}^n(I_1) = \widehat{T}(\widehat{T}^{n-1}(I_1))$ for $n \geq 1$. We transform this sequence into a binary sequence $a = a_1 a_2 \cdots a_n \cdots$ as follows. Define a binary function $\sigma : \mathcal{P}_m \to \{0,1\}$ by

$$\sigma(I_i) = \begin{cases} 1 & \text{for } I_i \subset (1/2, 1), \\ 0 & \text{for } I_i \subset (0, 1/2), \end{cases} \qquad i = 1, 2, \cdots, m. \tag{2}$$

We write $a_n = \sigma(\widehat{T}^{n-1}(I_1))$. Thus we obtain a binary sequence:

$$\begin{aligned} a &= a_1 a_2 \cdots a_n \cdots \\ &= \sigma(I_1)\sigma(\widehat{T}(I_1))\sigma(\widehat{T}^2(I_1)) \cdots \sigma(\widehat{T}^{n-1}(I_1)) \cdots. \end{aligned}$$

Apparently this sequence is periodic. If the least period of the sequence is $2m$, then the sequence is called the *maximal-length sequence* or the *full-length sequence*. Note that the obtained binary recurring sequence $a = a_1 a_2 \cdots a_n \cdots$ only depends on $\widehat{T}$. Hence we denote the maximal-length sequence by $\widehat{T}$. If $2m = 2^n$, then the maximal-length sequence is a complete cycle of length 2^n.

5. The Number of Maximal-Length Sequences

For $2m = 2^n$, then Theorem 2 by de Bruijn tells us that there are exactly $2^{2^{n-1}-n}$ maximal-length sequences in $\mathcal{T}_m$. For $2m \neq 2^n$, how many maximal-length sequences are there in $\mathcal{T}_m$ [5]? To answer this question, we require further results in graph theory.

Let G be a directed graph with vertices $v_1, v_2, \cdots, v_n$, and with a_{jk} arcs leading from v_j to v_k $(j, k = 1, 2, \cdots, n)$. The matrix $A = (a_{jk})$ $(1 \leq j, k \leq n)$ is called the *adjacency matrix*. Let $D = \mathrm{diag}(\mathrm{odeg}(v_1), \mathrm{odeg}(v_2), \cdots, \mathrm{odeg}(v_n))$. The matrix $C = D - A$ is called the *matrix of admittance*. An *oriented spanning tree* of G with root v_j is a set of $n-1$ arcs $a_1, a_2, \cdots a_{n-1}$ such that for $k = 1, 2, \cdots, n$, there is an directed path along these arcs from v_k to v_j. The following theorem is well-known as the matrix tree theorem.

Theorem 4 (Tutte [11]) *The number of oriented spanning trees of G with root v_j is the cofactor of C_{jj} in the matrix of admittance C.*

Theorem 5 (van Aardenne-Ehrenfest and de Bruijn [12]) *Let $G = (\mathcal{V}, \mathcal{A})$ be a directed graph with* odeg(v) =ideg(v) *for every vertex $v \in \mathcal{A}$, and let G' be an oriented spanning trees of G. Let r be the root of G' and let $a(v)$ be the arc of G' with initial vertex v. Let a_1 be with initial vertex r. Then $v_0 a_1 v_1 \cdots a_m v_m$, $v_0 = r, v_i \in \mathcal{V}$, $a_i = v_{i-1}v_i \in \mathcal{A}$ $(i = 1, 2, \cdots, m)$ is an Eulerian circuit if it is an oriented path for which*

i) no arc is used more than once.

ii) $a(v)$ is not used in $a_1, a_2, \cdots, a_m$ unless it is the only choice consistent with rule (i).

iii) $ra_1v_1 \cdots a_m v_m$ terminates only when it cannot be continued by rule (i).

By virtue of this theorem together with the matrix tree theorem, we obtain

Corollary 1 *For every $2m$, the number of maximal-length sequences in $\mathcal{T}_m$ is given by the cofactor of C_{11}*

in the matrix of admittance C obtained by the directed graph with m vertices and $2m$ arcs corresponding to the discretized dyadic transformation.

6. Entropy of the Discretized Dyadic Transformations

We may introduce a number-theoretic function associated with the numbers of maximal-period sequences based on the discretized dyadic transformations as follows. For $m = 1, 2, \cdots$, $\nu(m)$ is defined by the number of maximal-length sequences in $\mathcal{T}_m$. A short table of values of $\nu(m)$ is in the following:

m:	1	2	3	4	5	6	7	8	9	10
$\nu(m)$:	1	1	1	2	3	4	7	16	21	48

By the fundamental theorem of arithmetic, we can write $m = q2^s$ where $2 \not| q$. Thus Theorem 3 leads to

$$\nu(q2^s) = \nu(q)2^{q(2^s-1)-s}.$$

A short table of values of $\nu(q)$ is as follows:

q:	1	3	5	7	9	11	13	15	17
$\nu(q)$:	1	1	3	7	21	93	315	675	3825

We may also introduce

Definition 3 *The entropy h_m of the discretized dyadic transformations is defined by*

$$h_m = \frac{1}{L_m} \log \nu(m), \tag{3}$$

where $L_m = 2m$ is the the least period of the maximal-length sequence.

Remark 2 *Fix a positive odd integer q. For $m = q2^s$, we obtain*

$$h_m \to \frac{1}{2} \log 2 \quad (s \to \infty). \tag{4}$$

This value can be interpreted as the complexity of the doubling process from a given directed graph G to its arc digraph G^*.

7. Discretized Markov Transformations

For an irreducible, aperiodic Markov transformation T, given a Markov partition $\mathcal{P}$ with respect to T, corresponding each subinterval $I \in \mathcal{P}$ to one arc $a(I)$, we obtain the set $\mathcal{A}$ of arcs. For each ordered pair (I, J) of elements of $\mathcal{P}$, one vertex $v(I, J)$ adjacent from $a(I)$ and to $a(J)$ is allowed exactly when $J \subset T|_I(I)$. Thus we obtain the directed graph $G = (\mathcal{V}, \mathcal{A})$ representing the Markov transformation. Generally, this is not Eulerian. Further, we need the following notions in Graph theory.

A directed graph $H = (\mathcal{W}, \mathcal{B})$ is said to be a *subgraph* of the directed graph $G = (\mathcal{V}, \mathcal{A})$ if $\mathcal{W} \subset \mathcal{V}$ and $\mathcal{B} \subset \mathcal{A}$. In this case we write $H \subset G$. The directed graph H is called a *spanning subgraph* of G if $\mathcal{W} = \mathcal{V}$. Furthermore, if H is Eulerian, it is called *Eulerian subgraph spanning G*. We are interested in the spanning Eulerian subgraph of G with *maximal* number of arcs.

Under the above-mentioned one-to-one correspondence between $\mathcal{P}$ and $\mathcal{A}$, we obtain the partition $\mathcal{Q}$ which corresponds to $\mathcal{B}$. Then the discretized Markov transformation $\widehat{T}$ is defined by a permutation $\widehat{T} : \mathcal{Q} \to \mathcal{Q}$ with $\widehat{T}(I) \subset T|_I(I)$ for all $I \in \mathcal{Q}$. Eventually, the number of maximal-length sequences in the discretized Markov transformation is given by the cofactor of C_{11} in the matrix of admittance C of the Eulerian subgraph H spanning G with maximal number of arcs.

8. Conclusion

In this study, we defined discretized Markov transformations and found an algorithm to give the number of maximal-period sequences based on discretized Markov transformations.

References

[1] S.M. Ulam and J. von Neumann, "On combination of stochastic and deterministic processes," *Bull. Amer. Math. Soc.*, vol.53, p.1120, 1947.

[2] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic Complex Spreading Sequences for Asynchronous DS-CDMA Part I : System Modeling and Results", *IEEE Trans. Circuit Syst. I* vol.CAS-44, No.10, pp.937-947, 1997.

[3] D. Knuth, *The Art of Computer Programming*, vol. 2, 3rd ed., Addison-Wesley, 1997.

[4] N. Masuda and K. Aihara, "Chaotic cipher by finite-state baker's map", *Trans. of IEICE*, vol. 82-A, pp.1038–1046, 1999 (in Japanese).

[5] A. Tsuneda, Y. Kuga, and T. Inoue, "New Maximal-Period Sequences Using Extended Nonlinear Feedback Shift Registers Based on Chaotic Maps", *IEICE Trans. on Funda.*, vol. E85-A, pp.1327–1332, 2002.

[6] R. Hirota and D. Takahashi, *Discrete and Ultradiscrete Systems*, Kyoritsu Shuppan, 2003 (in Japanese).

[7] N. G. de Bruijn, "A Combinatorial Problem", *Nederl. Akad. Wetensch. Proc.*, vol. 49, pp.758–764, 1946.

[8] L. Euler, "Solutio problematis ad geometriam situs pertinensis", *Comm. Acad. Sci. Imper. Petropol.*, vol. 8, pp. 128–140, 1736.

[9] Harary and Norman, "Some Properties of Line Digraphs", *Rend. Circ. Math. Palermo*, vol. 9, pp. 161–168, 1960.

[10] C. Flye Sainte-Marie, "Solution to problem number 58", *L'Intermediare des Mathematiciens,* vol. 1, pp. 107–110, 1894.

[11] W. T. Tutte, "The dissection of equilateral triangles into equilateral triangles", *Proc. Cambridge Phil. Soc.*, vol. 44, pp. 463–482, 1948.

[12] T. van Aardenne-Ehrenfest and N. G. de Bruijn, "Circuits and trees in oriented linear graphs", *Simon Stevin*, vol. 28, pp. 203–217, 1951.