IEICE TRANS. FUNDAMENTALS, VOL.E88–A, NO.10 OCTOBER 2005

PAPER Special Section on Nonlinear Theory and its Applications

Discretized Markov Transformations—An Example of Ultradiscrete Dynamical Systems—

Hiroshi FUJISAKI[†a)], *Member*

SUMMARY 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 the discretized dyadic transformations and the discretized golden mean transformations. Then we find an algorithm to give the number of maximal-period sequences based on these discretized transformations. Moreover, we define a number-theoretic function related to the numbers of maximal-period sequences based on these discretized transformations. We also introduce the entropy of the maximal-period sequences based on these discretized transformations.

key words: *discretized Markov transformations, maximal-period sequences*

1. Introduction

It's been nearly six decades since Ulam and von Neumann pointed out that, given an initial value, the sequence of iterating a one-dimensional ergodic transformation, for instance a logistic transformation: $T(x) = 4x(1 - x)$, is a good candidate for 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 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 [2]–[4] and as real-valued keystreams in so called chaotic encryption systems [5]. Unfortunately, however, they are not available for practical use.

To begin with, Ulam and von Neumann's idea requires handling real numbers in its applications. 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 [6].

Recently a breakthrough has been made as follows: Discretized Bernoulli transformations were considered and their applications to cryptography and SSMA communication systems were proposed [7], [8]. 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* [9]. 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 [8], maximal-period sequences based on discretized Bernoulli transformations were proposed and their correlational properties were numerically investigated. It is pointed out in [8] 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 [10], the numbers of maximal-period sequences based on several discretized Bernoulli transformations were numerically conjectured in [8]. Recently discretized Bernoulli transformations with negative autocorrelations, which are known to be optimum in terms of the average interference parameter (AIP) (see [4] for instance), are designed in [11].

In this report, we define discretized Markov transformations and find an algorithm to give the number of maximal-period sequences based on discretized Markov transformations. As concrete examples, we firstly focus on the dyadic transformation and the golden mean transformation, and define the discretized versions of these transformations. Then we find an algorithm to give the number of maximal-period sequences based on these discretized transformations. This includes a proof to Tsuneda et al.'s numerical conjecture on the numbers of maximal-period sequences based on discretized Bernoulli transformations. Moreover, we define a number-theoretic function related to the numbers of maximal-period sequences based on these discretized transformations. We also introduce the entropy of the maximal-period sequences based on these discretized transformations. We note here that recently Lyapunov exponents for permutations are defined in [12]. Finally we generalize these two examples and define the discretized Markov transformations and show an algorithm to give the number of maximal-period sequences based on discretized Markov transformations.

Manuscript received January 18, 2005.
Final manuscript received June 6, 2005.

[†]The author is with the Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa-shi, 920-1192 Japan.
a) E-mail: fujisaki@t.kanazawa-u.ac.jp

DOI: 10.1093/ietfec/e88–a.10.2684

*Especially the notion of *ultradiscrete dynamical systems* was proposed by Professor Shunji Ito.

This report is composed of seven sections. In Sect. 2, we point out that de Bruijn sequences are originally related to number-theoretic sequences called normal recurring sequences [13]. In Sect. 3, we briefly summarize de Bruijn's results on the number of normal recurring sequences. In Sects. 4 and 5, we focus on the dyadic transformation and the golden mean transformation, and we define the discretized versions of these transformations. Then we find an algorithm to give the number of maximal-period sequences based on these discretized transformations. We define a number-theoretic function related to the numbers of maximal-period sequences based on these discretized transformations. We also introduce the entropy of the maximal-period sequences based on these discretized transformations. In Sect. 6, we generalize these two examples and define the discretized Markov transformations and give an algorithm to give the number of maximal-period sequences based on discretized Markov transformations. The report concludes with the summary in Sect. 7.

2. Preliminaries

2.1 Normal Recurring Sequence

Let $x \in (0,1)$. We suppose x is expressed in the dyadic expansion as

$$x = \frac{x_1}{2} + \frac{x_2}{2^2} + \cdots, \quad x_i \in \{0,1\} \quad (i = 1,2,\cdots). \qquad (1)$$

We simply write this as $x = x_1 x_2 \cdots$.

For the digit $b(\in \{0,1\})$, we denote the number of occurrences of b in the first n places in x by n_b. If $n_b/n \to p_b$ when $n \to \infty$, then we say that b has *frequency* p_b in x. We say that x is *simply normal* if $n_b/n \to 1/2$ for each b.

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 $\{0,1\}^n$.

Similarly, for a binary k-word b, we denote the number of occurrence of b in the first n places in x by n_b. If $n_b/n \to 1/2^k$ when $n \to \infty$, then we say that b has *normal frequency* in x. We say that x has *normality of order k* if $n_b/n \to 1/2^k$ as $n \to \infty$ for all $b \in \{0,1\}^k$.

If x has normality of order k for all positive integers k then it is said to be *normal*.

Theorem 1 (Borel [14]): Almost all numbers are normal.

Remark 1: No rational number can be normal.

For a given positive integer k, the question arises whether there are recurring binary sequences with normality of order k.

Theorem 2 (Good [13]): There is a recurring binary sequence of period 2^k which has normality of order k.

The proof employs an analogue of Euler's unicursal theorem.

2.2 Euler's Unicursal Theorem

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: $v_0 e_1 v_1 \cdots e_n v_n$, $v_{i-1}, v_n \in \mathcal{V}$, $e_i = \{v_{i-1}, v_i\} \in \mathcal{E}$ $(i = 1,2,\cdots,n)$. 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 3 (Euler [15]): A graph G is Eulerian if and only if it is connected and every vertex has an even degree.

2.3 An Eulerian Circuit in a Directed Graph

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 $v_0 a_1 v_1 \cdots a_n v_n$, $v_{i-1}, v_n \in \mathcal{V}$, $a_i = v_{i-1} v_i \in \mathcal{A}$ $(i = 1,2,\cdots,n)$. If $v_0 = v_n$, then the 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.

It is worth noting that Good proved Theorem 2 by using the notion of so-called *edge shift* in symbolic dynamics†. We give here the sketch of Proof of Theorem 2:

Let $k > 1$. Any binary $(k-1)$-word is defined as a vertex. For two vertices of the forms $u = a_1 a_2 \cdots a_{k-1}$, $v = a_2 a_3 \cdots a_k$, the binary k-word $a = a_1 a_2 \cdots a_k$ is defined as an arc from u to v. We obtain 2^k distinct arcs

†In symbolic dynamics, the arc defined here is called the edge [18].

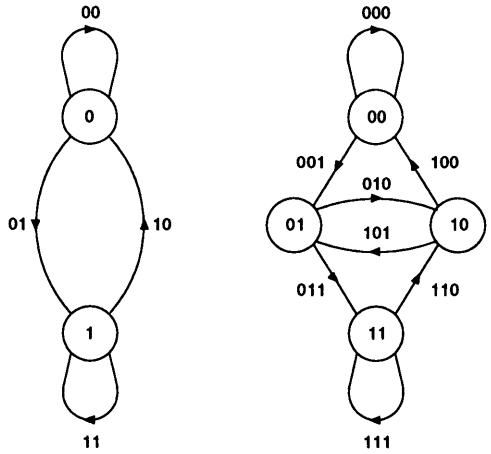


Fig. 1 Graphs of G_2 and G_3.

from 2^{k-1} vertices. We denote the set of all vertices and the set of all arcs by $\mathcal{V}_k = \{0,1\}^{k-1}$ and $\mathcal{A}_k = \{0,1\}^k$ respectively. Thus we obtain a directed graph $G_k = (\mathcal{V}_k, \mathcal{A}_k)$. Graphs of G_2 and G_3 are shown in Fig. 1. For every vertex v, we have odeg(v) =ideg(v) = 2. The directed graph G is connected since for any two vertices $a_1a_2\cdots a_{k-1}$ and $b_1b_2\cdots b_{k-1}$ a word $a_1a_2\cdots a_{k-1}b_1b_2\cdots b_{k-1}$ corresponds to a walk $a_1\cdots a_{k-1}(a_1\cdots a_{k-1}, a_2\cdots a_{k-1}b_1)a_2\cdots a_{k-1}b_1\cdots$ $\cdots(a_{k-1}b_1\cdots b_{k-2}, b_1\cdots b_{k-1})b_1\cdots b_{k-1}$. Thus there exists an Eulerian circuit in the directed graph G_k, which provides a recurring binary sequence of period 2^k which has normality of order k.

3. De Bruijn Sequences

A (*binary*) *cycle* of length k is a sequence of k digits $a_1a_2\cdots a_k$ taken in a circular order. In the cycle $a_1a_2\cdots a_k$, a_1 follows a_k, and $a_2\cdots a_ka_1, \cdots, a_ka_1\cdots a_{k-1}$ are all the same cycle as $a_1a_2\cdots a_k$.

A (*binary*) *complete cycle* of length 2^n is a cycle of binary 2^n-words, 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. A complete cycle of length 2^n has normality of order n.

Example 1: We give examples of complete cycles of length 2^n:

$n = 1$, 01,
$n = 2$, 0011,
$n = 3$, 00010111,
00011101.

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

Theorem 4 (de Bruijn [10], Flye Sainte-Marie [17]): 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

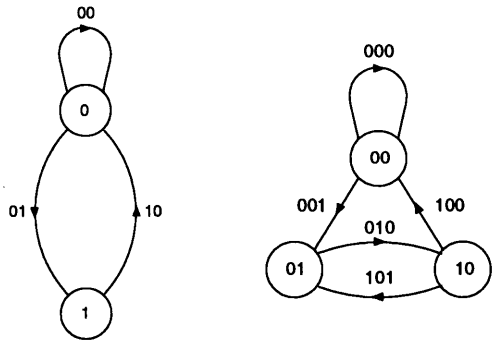


Fig. 2 An example of a directed graph G and its arc digraph G^*.

Theorem 5 (de Bruijn [10]): Let G be a directed graph with m vertices such that odeg(v) =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 4 enables us to determine the number of k-ary complete cycles:

Remark 2: For each positive integer n, there are exactly $\{(k-1)!\}^{k^{n-1}}k^{k^{n-1}-n}$ complete cycles of length k^n.

To prove Theorem 4, de Bruijn introduced the *arc digraph* of an given digraph†.

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

$$\sigma_j = \sum_{k=1}^{n} a_{jk} = \text{odeg}(v_j); \tag{2}$$

$$\tau_k = \sum_{j=1}^{n} a_{jk} = \text{ideg}(v_k). \tag{3}$$

Definition 1: (de Bruijn [10], Harary and Norman [16]) 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 $k = j'$.

An example of a directed graph G and its arc digraph G^* is shown in Fig. 2.

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.

Let $G_n = (\mathcal{V}_n, \mathcal{A}_n)$ $(n > 1)$ be a directed graph introduced by Good. That is $\mathcal{V}_n = \{0,1\}^{n-1}$ and $\mathcal{A}_n = \{0,1\}^n$, and an arc $a_1a_2\cdots a_n \in \mathcal{A}$ goes from $a_1a_2\cdots a_{n-1}$ to $a_2a_3\cdots a_n$. The most important part of de Bruijn's proof lies in the recognition of a relation between the graphs G_n and G_{n+1}:

$$G_{n+1} = G_n^*, \tag{4}$$

†In symbolic dynamics, the arc digraph is called the *2nd higher edge graph* [18].

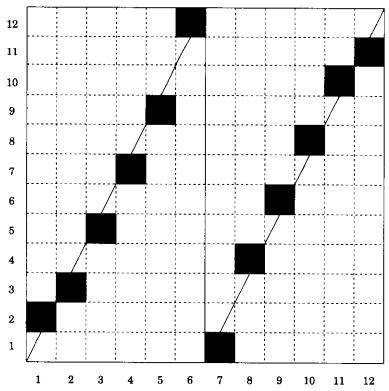


Fig. 3 An example of discretized dyadic transformations. ($m = 6$)

where G_n^* is the arc digraph of G_n. From this relation and the fact that G_2 has exactly one complete cycle, the theorem follows by induction on n from Theorem 5.

4. Discretized Dyadic Transformations

4.1 Markov Partition

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.

4.2 Discretized Dyadic Transformations

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 2: 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 3 shows the discretized dyadic transformation $\widehat{T}$.

This permutation can be represented by binary 6-word 100001 corresponding to 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

$$a_i = \begin{cases} 1 & \text{for } \widehat{T}(I_i) = I_{2i}, \\ 0 & \text{for } \widehat{T}(I_i) = I_{2i-1}, \end{cases} \quad i = 1, 2, \cdots, m. \quad (5)$$

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

$$\sigma(I_i) = \begin{cases} 1 & \text{for } I_i \subset (1/2, 1), \\ 0 & \text{for } I_i \subset (0, 1/2), \end{cases} \quad i = 1, 2, \cdots, m. \quad (6)$$

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

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

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.

4.3 The Number of Maximal-Length Sequences

For $2m = 2^n$, then Theorem 4 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 $\mathcal{T}_m$ [8]? 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 $A = (a_{jk})_{j,k=1}^n$ 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 a directed path along these arcs from v_k to v_j. The following theorem is well-known as the matrix tree theorem.

Theorem 6 (Tutte [19]): The number of oriented spanning trees of G with root v_j is the cofactor of C_{jj} in the matrix of admittance C.

Example 3: Let us consider a directed graph shown in Fig. 4. Its matrix of admittance is given by

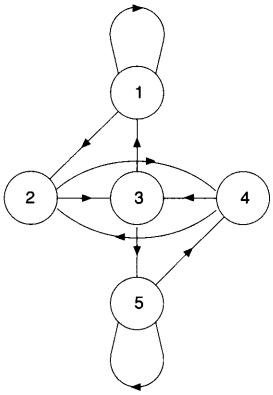


Fig. 4 A directed graph.

$$C = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 2 & -1 & -1 & 0 \\ -1 & 0 & 2 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix}$$

The cofactor of C_{11} in C is 3. We can easily confirm the number of oriented subtrees of the graph in Fig. 4 is also 3.

Theorem 7: (van Aardenne-Ehrenfest and de Bruijn [20]) 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 tree 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 any arc 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 m, the number of maximal-length sequences in $\mathcal{T}_m$ is given by the cofactor of C_{11} in the matrix of admittance C of the directed graph with m vertices and $2m$ arcs corresponding to the discretized dyadic transformation.

4.4 A Number-Theoretic Function ν

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 $2 \nmid q$. If an integer a is divisible by another integer $b\,(\neq 0)$, we denote it by $b \mid a$. Unless a is divisible by b, we denote it by $b \nmid a$. Thus Theorem 5 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

4.5 Entropy of the Discretized Dyadic Transformations

We may also introduce

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

$$h_m = \frac{1}{L_m} \log \nu(m), \tag{7}$$

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

Remark 3: Choose a positive odd integer q. For $m = q2^s$, we obtain

$$h_m \to \frac{1}{2} \log 2 \quad (s \to \infty). \tag{8}$$

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

5. Discretized Golden Mean Transformations

5.1 Markov Partition of Golden Mean Transformation

Let $T : [0, 1] \to [0, 1]$ be the golden mean transformation:

$$T(x) = \beta x \pmod 1, \quad x \in [0, 1],$$

where β is the golden mean number $\frac{1+\sqrt{5}}{2}$. To construct a Markov partition with respect to T, consider a set of binary n-words in which the word 11 does not appear as a subword, and denote it by $\mathcal{B}_n$.

Example 4: Examples of $\mathcal{B}_n$:

$\mathcal{B}_1 = \{0, 1\}$,
$\mathcal{B}_2 = \{00, 01, 10\}$,
$\mathcal{B}_3 = \{000, 001, 010, 100, 101\}$,
$\mathcal{B}_4 = \{0000, 0001, 0010, 0100, 0101, 1000, 1001, 1010\}$.

Note that $\#\mathcal{B}_n$ is the *Fibonacci numbers* which is the sequence of numbers $(\#\mathcal{B}_n)_{n\in\mathbb{N}}$ with $\#\mathcal{B}_1 = 2$, $\#\mathcal{B}_2 = 3$, and

$$\#\mathcal{B}_{n+2} = \#\mathcal{B}_{n+1} + \#\mathcal{B}_n.$$

Let $\mathcal{B}_n$ be equipped with a total order relation $\leq$ defined by the following: for any n-words $a = a_1a_2 \cdots a_n$, $a' = a'_1a'_2 \cdots a'_n \in \mathcal{B}_n$, $a \leq a'$ iff

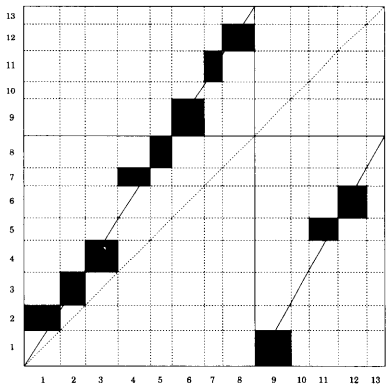


Fig. 5 An example of discretized golden mean transformations ($n = 5$).

$$a_1\beta^{n-1}+a_2\beta^{n-2}+\cdots+a_n \le a'_1\beta^{n-1}+a'_2\beta^{n-2}+\cdots+a'_n.$$

Thus we can number all the elements in $\mathcal{B}_n$:

$$a^{(0)} < a^{(1)} < \cdots < a^{(\#\mathcal{B}_n-1)}.$$

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

$$0 = p_0 < p_1 < p_2 < \cdots < p_{\#\mathcal{B}_n-1} < 1,$$

where

$$p_i = \frac{1}{\beta^n}\left(a_1^{(i)}\beta^{n-1} + a_2^{(i)}\beta^{n-2} + \cdots + a_n^{(i)}\right),$$

$i = 0, 1, 2, \cdots, \#\mathcal{B}_n - 1$. For $i = 1, \cdots, \#\mathcal{B}_n$, let $I_i = (p_{i-1}, p_i)$ where $p_{\#\mathcal{B}_n} = 1$. Thus the partition $\mathcal{P}_n = \{I_i\}_{i=1}^{\#\mathcal{B}_n}$ is a Markov partition with respect to T.

Example 5: We give an example of discretized golden mean transformations ($n = 5$):

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

Figure 5 shows the discretized golden mean transformation $\widehat{T}$.

Note that the subintervals I_{10} and I_{13} are excluded from $\mathcal{P}_5$[†].

This permutation can be represented by binary 3-word 101 corresponding to the relation between I_i and $\widehat{T}(I_i)$ for $i = 1, 3, 4$. And hence for $n = 5$ the total number of the discretized golden mean transformations is 8.

5.2 Eulerian Subgraph Spanning G and Discretized Golden Mean Transformations

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. Figure 6 shows an example of a directed graph and its spanning Eulerian subgraph with maximal number of arcs.

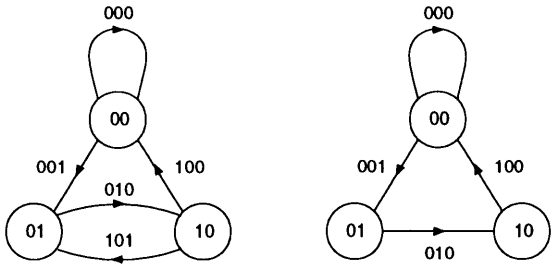


Fig. 6 An example of a directed graph and its spanning Eulerian subgraph with maximal number of arcs.

Let $k > 1$. Any binary $(k-1)$-word in $\mathcal{B}_{k-1}$is defined as a vertex. For two vertices of the forms $u = a_1a_2\cdots a_{k-1}$, $v = a_2a_3\cdots a_k$, the binary k-word $a = a_1a_2\cdots a_k$ is defined as an arc from u to v. We obtain $\#\mathcal{B}_k$ distinct arcs from $\#\mathcal{B}_{k-1}$ vertices. We denote the set of all vertices and the set of all arcs by $\mathcal{V}_k = \mathcal{B}_{k-1}$ and $\mathcal{A}_k = \mathcal{B}_k$ respectively. Thus we obtain a directed graph $G_k = (\mathcal{V}_k, \mathcal{A}_k)$, which has the following property:

Property 1: For every vertex v, we have

$$\begin{aligned} &\mathrm{odeg}(v) = \mathrm{ideg}(v) = 2 \quad \text{if} \quad v = 0v_2v_3\cdots v_{k-2}0, \\ &\mathrm{odeg}(v) = \mathrm{ideg}(v) = 1 \quad \text{if} \quad v = 1v_2v_3\cdots v_{k-2}1, \end{aligned}$$

as well as

$$\begin{aligned} &\mathrm{odeg}(v) = 1,\ \mathrm{ideg}(v) = 2 \quad \text{if} \quad v = 0v_2v_3\cdots v_{k-2}1, \\ &\mathrm{odeg}(v) = 2,\ \mathrm{ideg}(v) = 1 \quad \text{if} \quad v = 1v_2v_3\cdots v_{k-2}0. \end{aligned}$$

By virtue of Theorem 2 by Good, we obtain

Lemma 1: Exclude all arcs in the form of $a = 1a_2a_3\cdots a_{k-1}1$ from $\mathcal{A}_k$ and denote the set of the rest of arcs in $\mathcal{A}_k$ by $\mathcal{E}_k$, then the directed graph $H_k = (\mathcal{V}_k, \mathcal{E}_k)$ is the spanning Eulerian subgraph of G_k with *maximal* number of arcs.

Note that $\#\mathcal{E}_k = \#\mathcal{B}_k - \#\mathcal{B}_{k-3}$ $(k > 3)$ and the sequence $(\#\mathcal{E}_k)_{k=3}^{\infty}$ is also the Fibonacci numbers with $\#\mathcal{E}_3 = 4$ and $\#\mathcal{E}_4 = 6$.

Obviously $\mathcal{P}_n$ and $\mathcal{A}_n$ are in one-to-one correspondence. Let $\mathcal{Q}_n$ be the partition which corresponds to $\mathcal{E}_n$ under this one-to-one correspondence. We take $\mathcal{E}_n$ as the index set to its corresponding partition $\mathcal{Q}_n$. Then we can define the discretized golden mean transformations as follows.

Definition 4: For each n, the discretized golden mean transformation $\widehat{T}$ is defined by a permutation $\widehat{T} : \mathcal{Q}_n \to \mathcal{Q}_n$ with $\widehat{T}(I_b) \subset T|_{I_b}(I_b)$ for $b \in \mathcal{E}_n$.

We denote the set of all discretized golden mean transformations by $\mathcal{T}_n$.

Note that $\#\mathcal{T}_n = 2^{\#\mathcal{B}_{n-3}}$, where $\mathcal{B}_{-2} = 0$ and $\mathcal{B}_{-1} = 1$. Let $\widehat{T} \in \mathcal{T}_n$. We define a bijection $\phi : \mathcal{T}_n \to \{0,1\}^{\#\mathcal{B}_{n-3}}$ by $\phi(\widehat{T}) = b_1b_2\cdots b_{\#\mathcal{B}_{n-3}}$ as follows.

[†]This fact was pointed out in [21].

For $n = 2$,

$$b_1 = \begin{cases} 0 & \text{if } \widehat{T}(I_{00}) = I_{00}, \\ 1 & \text{if } \widehat{T}(I_{00}) = I_{01}. \end{cases}$$

For $n > 2$,

$$b_i = \begin{cases} 0 \text{ if } \widehat{T}(I_{00a_3a_4\cdots a_{\#\mathcal{B}_{n-1}}0}) = I_{0a_3a_4\cdots a_{\#\mathcal{B}_{n-1}}00}, \\ 1 \text{ if } \widehat{T}(I_{00a_3a_4\cdots a_{\#\mathcal{B}_{n-1}}0}) = I_{0a_3a_4\cdots a_{\#\mathcal{B}_{n-1}}01}, \end{cases}$$

$i = 1, 2, \cdots, \#\mathcal{B}_{n-3}$.

For a given binary $\#\mathcal{B}_{n-3}$-word b, we simply write $\phi^{-1}(b) = \widehat{T}_b$.

5.3 Maximal-Length Sequences

Let $\widehat{T} \in \mathcal{T}_n$. Consider a sequence of subintervals from $\mathcal{Q}_n$: $(\widehat{T}^k(I_{0\cdots0}))_{k=0}^{\infty}$ where $\widehat{T}^0(I_{0\cdots0}) = I_{0\cdots0}$ and $\widehat{T}^k(I_{0\cdots0}) = \widehat{T}(\widehat{T}^{k-1}(I_{0\cdots0}))$ for $k \geq 1$. We transform this sequence into a binary sequence $a = a_1a_2\cdots a_k\cdots$ as follows. Define a binary function $\sigma : \mathcal{Q}_n \to \{0, 1\}$ by

$$\sigma(I_b) = \begin{cases} 1 & \text{for } I_b \subset (1/\beta, 1), \\ 0 & \text{for } I_b \subset (0, 1/\beta), \end{cases} \qquad b \in \mathcal{E}_n. \tag{9}$$

We write $a_k = \sigma(\widehat{T}^{k-1}(I_{0\cdots0}))$. Thus we obtain a binary sequence:

$$\begin{aligned} a &= a_1a_2\cdots a_k\cdots \\ &= \sigma(I_{0\cdots0}), \sigma(\widehat{T}(I_{0\cdots0}))\sigma(\widehat{T}^2(I_{0\cdots0}))\cdots \\ &\quad \cdots\sigma(\widehat{T}^{k-1}(I_{0\cdots0}))\cdots. \end{aligned}$$

This sequence is periodic. If the least period of the sequence is $\#\mathcal{E}_n$, then the sequence is called the *maximal-length sequence* or the *full-length sequence*. Note that the obtained binary recurring sequence $a = a_1a_2\cdots a_k\cdots$ only depends on $\widehat{T}$. Hence we denote the maximal-length sequence by $\widehat{T}$.

Corollary 2: For every n, the number of maximal-length sequences in $\mathcal{T}_n$ is given by the cofactor of C_{11} in the matrix of admittance C of the Eulerian subgraph H_n spanning G_n with *maximal* number of arcs, where $G_n = (\mathcal{B}_{n-1}, \mathcal{B}_n)$ is the directed graph corresponding to the discretized golden mean transformation.

We denote the the number of maximal-length sequences in $\mathcal{T}_n$ by M_n.

A short table of values of M_n:

n:	1	2	3	4	5	6	7	8	9
M_n :	1	1	1	1	2	2	28	216	65200

We need the relation between M_n and M_{n+1} to obtain an explicit formula for the nth term. Unfortunately, however, we cannot apply Theorem 5 by de Bruijn since $H_n^* \subset_{\neq} H_{n+1}$.

5.4 Entropy of Discretized Golden Mean Transformations

We may introduce

Definition 5: The entropy h_n of the discretized golden mean transformations is defined by

$$h_n = \frac{1}{\#\mathcal{E}_n} \log M_n. \tag{10}$$

A short table of values of h_n:

n:	3	4	5	6	7	8	9
h_n :	0	0	0.0693	0.0433	0.1281	0.1279	0.1630

Conjecture 1: We may expect

$$\lim_{n\to\infty} \frac{1}{\#\mathcal{E}_n} \log M_n = \frac{1}{\beta} \log\beta (= 0.2546...). \tag{11}$$

If this conjecture is proved, then this result can be generalized to the class of shifts of finite type considering a sequence of higher arc (edge) graphs.

6. Discretized Markov Transformations

In this section, we generalize the above-mentioned two examples of discretized transformations and define the 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.

7. 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. As concrete examples, we focused on the discretized dyadic transformations and the discretized golden mean transformations. Then we found an algorithm to give the

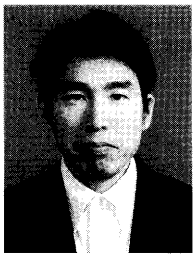
number of maximal-period sequences based on these discretized transformations. Moreover, we defined a number-theoretic function related to the numbers of maximal-period sequences based on these discretized transformations. We also introduced the entropy of the maximal-period sequences based on these discretized transformations.

Acknowledgment

The author is grateful to Professor Shunji Ito in the Graduate School of Natural Science and Technology, Kanazawa University, Japan for his encouragement. The author also thanks Professor Roger R. Anderson in the Department of Physics and Astronomy, the University of Iowa, USA for his helping the author's English writings.

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. Heidari-Bateni, C.D. McGillem, and M.F. Tenorio, "A novel multiple-address digital communication system using chaotic signals," Proc. 1992 IEEE International Conference on Communications (ICC'92), pp.1232–1236, 1992.
[3] T. Kohda, A. Tsuneda, and T. Sakae, "Chaotic binary sequences by Chebyshev maps and their correlation properties," Proc. IEEE Second Int. Symp. on Spread Spectrum Techniques and Applications, pp.63–66, 1992.
[4] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA Part I: System modeling and results," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.44, no.10, pp.937–947, 1997.
[5] M. Götz, K. Kelber, and W. Schwarz, "Discrete-time chaotic encryption systems Part I: Statistical design approach," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.44, no.10, pp.963–970, 1997.
[6] D. Knuth, The Art of Computer Programming, vol.2, 3rd ed., Addison-Wesley, 1997.
[7] N. Masuda and K. Aihara, "Chaotic cipher by finite-state baker's map," IEICE Trans. Fundamentals (Japanese Edition), vol.J82-A, no.7, pp.1038–1046, July 1999.
[8] A. Tsuneda, Y. Kuga, and T. Inoue, "New maximal-period sequences using extended nonlinear feedback shift registers based on chaotic maps," IEICE Trans. Fundamentals, vol.E85-A, no.6, pp.1327–1332, June 2002.
[9] R. Hirota and D. Takahashi, Discrete and Ultradiscrete Systems, Kyoritsu Shuppan, 2003.
[10] N.G. de Bruijn, "A combinatorial problem," Nederl. Akad. Wetensch. Proc., vol.49, pp.758–764, 1946.
[11] D. Yoshioka, A. Tsuneda, and T. Inoue, "Maximal-period sequences with negative auto-correlations and their application to asynchronous DS-CDMA systems," IEICE Trans. Fundamentals, vol.E86-A, no.6, pp.1405–1413, June 2003.
[12] L. Kocarev and J. Szczepanski, "Finite-space Lyapunov exponents and pseudochaos," Phys. Rev. Lett., vol.93, 234101, 2004.
[13] I.J. Good, "Normal recurring decimals," J. London Math. Soc., vol.21, pp.167–172, 1946.
[14] E. Borel, "Les probabilités dé nombrables et leurs applications arithmétiques," Rend. Circ. Mat. Palermo, vol.27, pp.247–271, 1909.
[15] L. Euler, "Solutio problematis ad geometriam situs pertinensis," Comm. Acad. Sci. Imper. Petropol., vol.8, pp.128–140, 1736.
[16] F. Harary and R.Z. Norman, "Some properties of line digraphs," Rend. Circ. Math. Palermo, vol.9, pp.161–168, 1960.
[17] C.F. Sainte-Marie, "Solution to problem number 58," L'Intermediare des Mathematiciens, vol.1, pp.107–110, 1894.
[18] D. Lind and B. Marcus, Symbolic Dynamics and Coding, Cambridge Univ. Press, 1995.
[19] W.T. Tutte, "The dissection of equilateral triangles into equilateral triangles," Proc. Cambridge Phil. Soc., vol.44, pp.463–482, 1948.
[20] T. van Aardenne-Ehrenfest and N.G. de Bruijn, "Circuits and trees in oriented linear graphs," Simon Stevin, vol.28, pp.203–217, 1951.
[21] F. Enomoto, "Discretization of transformations and maximal periodic sequences," Workshop on Number Theory and Ergodic Theory, Kanazawa, April 2004.



Hiroshi Fujisaki is a lecturer of the Graduate School of Natural Science and Technology, Kanazawa University, Ishikawa, Japan. He received the B.E. and M.E. degrees in Electronic Engineering from Kyushu University, Fukuoka, Japan, in 1989 and 1991 respectively. He received the D.E. degree in Communication Engineering from the Department of Computer Science and Communication engineering, Kyushu University, Fukuoka, Japan in 2001. From 1991 to 1996, he worked as a Research Staff in Hitachi, Ltd., Ibaraki, Japan. From 1998 to 2001, he worked as a Research Associate in the Department of Computer Science and Communication engineering, Kyushu University. His research interests are in statistical properties of one-dimensional transformations and their applications to digital communication systems.