2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Correlatinal Properties of the Full-Length Sequences Based on the Discretized Golden Mean Transformations

Hiroshi Fujisaki

Graduate School of Natural Science and Technology
Kanazawa University
Kakuma-machi, Kanazawa, Ishikawa, 920-1192 Japan
Email: fujisaki@t.kanazawa-u.ac.jp

Abstract—We have previously defined the discretized Markov transformations and the full-length sequences based on such transformations. In this report, the focus is on the discretized golden mean transformation. In view of basic properties of the correlation functions for the de Bruijn sequences that can be regarded as the full-length sequences based on the discretized dyadic transformation, we obtain such basic properties of the correlation functions for the full-length sequences based on the discretized golden mean transformation.

1. Introduction

Discretized Bernoulli transformations are proposed for cryptography and spread-spectrum multiple access (SSMA) communication systems in [1] and [2] respectively. Motivated by these results, we defined discretized Markov transformations and found an algorithm to give the number of full-length sequences based on the discretized Markov transformations in [3].

In [4], we defined the piecewise-monotone-increasing Markov transformations, which included not only Bernoulli transformations but also Markov β transformations, and gave the bounded monotone truth-table algorithm for generating *all* full-length sequences which were based on the discretized piecewise-monotone-increasing Markov transformations.

Although correlational properties of pseudo-random sequences play important roles in cryptography and SSMA communication systems, it is intractable to characterize the correlational properties of full-length sequences based on the discretized piecewise-monotone-increasing Markov transformations because of the nature of nonlinearity. Even for the de Bruijn sequences, only bounds of the maximum values of the normalized auto-correlation functions had been known [5]. In [6], we have provided a novel lower bound of the minimum values of the normalized auto-correlation functions for the de Bruijn sequences of length 2^n ($n \geq 3$). Furthermore, from the view point of symbolic dynamics [7]–[8], we solved in [10]–[11] the fundamental problem posed by Fredricksen in [9] on existence of the CR (complement reverse) sequences in the de Bruijn sequences of length 2^n for any odd n.

In this report, we focus on the golden mean transformation, which is the simplest but nontrivial example of Markov β transformations, and we obtain basic properties of the correlation functions for the full-length sequences based on the discretized golden mean transformation.

This report is composed of six sections. In Sect. 2, we introduce the shift space and define the topological Markov chain from symbolic dynamics [7]–[8]. In Sect. 3, we review the discretized Markov transformations defined in [3]. Then we check that the de Bruijn sequences are the full-length sequences based on the discretized dyadic transformation. In Sect. 4, we introduce the correlation functions and recall basic properties of the correlation functions for the de Bruijn sequences. In Sect. 5, in the light of well known properties of the correlation functions for the de Bruijn sequences, we obtain such basic properties of the correlation functions for the full-length sequences based on the discretized golden mean transformation. The report concludes with the summary in Sect. 6.

2. Preliminaries

Let Σ be a finite alphabet. The full Σ-shift is denoted by

$$\Sigma^{\mathbb{Z}} = \{x = (x_i)_{i\in\mathbb{Z}} : \forall i \in \mathbb{Z},\ x_i \in \Sigma\}$$

which is endowed with the product topology arising from the discrete topology on Σ. The shift transformation $\sigma : \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ is defined by

$$\sigma((x_i)_{i\in\mathbb{Z}}) = (x_{i+1})_{i\in\mathbb{Z}}.$$

The closed shift-invariant subsets of $\Sigma^{\mathbb{Z}}$ are called subshifts. For a subshift X, we use σ_X to denote the shift transformation on X, which is the restriction to X of σ on $\Sigma^{\mathbb{Z}}$. For simplicity, we shall write $\sigma : X \to X$ rather than σ_X.

We call elements $u = u_1u_2\cdots u_n \in \Sigma^n$ blocks over Σ of length n ($n \geq 1$). We use Σ^* to denote the collection of all blocks over Σ and the empty block ϵ. For a subshift X, we use $\mathcal{L}_n(X)$ to denote the collection of all n-blocks appearing in points in X. The language of X is the collection $\mathcal{L}(X) = \bigcup_{n=0}^{\infty} \mathcal{L}_n(X)$, where $\mathcal{L}_0(X) = \{\epsilon\}$.

A (directed) graph $G = (\mathcal{V}, \mathcal{A})$ consists of a finite set $\mathcal{V}$ of *vertices* and a finite set $\mathcal{A}$ of *edges*. Each edge $e \in \mathcal{A}$

starts at a vertex called *initial state* denoted by $\mathbf{i}(e) \in \mathcal{V}$ and *terminates* at a vertex called *terminal state* denoted by $\mathbf{t}(e) \in \mathcal{V}$.

Definition 1 *Let $G = (\mathcal{V}, \mathcal{A})$ be a graph. For vertices $u, v \in \mathcal{V}$, let $a_{u,v}$ denote the number of edges in G with initial state u and terminal state v. Then the adjacency matrix of G is $A = (a_{u,v})_{u,v\in\mathcal{V}}$, and its formation from G is denoted by $A = A(G)$ or $A = A_G$. Conversely, $k\times k$ nonnegative integral matrix $B = (b_{i,j})_{i,j=0}^{k-1}$ determines a graph H with vertex set $\{0, 1, \cdots, k-1\}$ and $a_{i,j}$ distinct edges with initial state i and terminal state j, and its formation from B denoted by $H = G(B)$ or $H = G_B$. It is worth noting that $A = A(G_A)$ and that G and $H = G(A_G)$ are graph isomorphic.*

For a given nonnegative integral matrix A, we set $G_A = (\mathcal{V}, \Sigma)$. Let

$$X_A = \{(x_n)_{-\infty}^{\infty} \in \Sigma^{\mathbb{Z}} : \mathbf{t}(x_n) = \mathbf{i}(x_{n+1}) \text{ for all } n \in \mathbb{Z}\}.$$

Then $\sigma : X_A \to X_A$ is called the two-sided topological Markov chain determined by the matrix A. The topological Markov chain is also called a subshift of finite type (SFT) since it can be described by a finite set of forbidden blocks. For a given finite set $\mathcal{F}$ of forbidden blocks, we use $X_{\mathcal{F}}$ to denote the SFT.

3. Discretized Markov Transformations

We first recall the definition of the discretized Markov transformations defined in [3] as follows.

Definition 2 *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.*

We use $|E|$ to denote the cardinality of a set E.

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 edge $e(I)$, we obtain the set $\mathcal{A}$ of edges. For each ordered pair (I, J) of elements of $\mathcal{P}$, one vertex $v(I, J)$ adjacent from $e(I)$ and to $e(J)$ is allowed exactly when $J \subset T|_I(I)$. Thus we obtain the graph $G = (\mathcal{V}, \mathcal{A})$ representing the Markov transformation. Generally, this is not Eulerian.

Let $H = (\mathcal{V}, \mathcal{B})$ be the Eulerian subgraph spanning G with maximal number of edges. Since we consider the irreducible aperiodic Markov transformations, the set $\mathcal{V}$ of vertices is invariant under the modification from G to H. 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 $I \in \mathcal{Q}$.

Full-length sequences based on the discretized Markov transformation are exactly Eulerian circuits in H, whose length is given by $|\mathcal{B}|$. Given a Markov partition $\mathcal{P}$ with respect to T, we obtain $|\mathcal{Q}|!$ discretized Markov transformations. It is well known that any permutation is uniquely expressible (except for the order of succession) as a product of cyclic permutations. In view of this fact, the discretized Markov transformation $\widehat{T} : \mathcal{Q} \to \mathcal{Q}$ can be regarded as an approximation of the underlying transformation $T : [0, 1] \to [0, 1]$ only when it is expressed as precisely one cyclic permutation. In such cases, the discretized Markov transformation $\widehat{T}$ itself can be viewed as a full-length sequence w. Moreover, for the full-length sequence w, considering a bi-infinite sequence $w^{\infty} = \cdots www \cdots$, the cyclic permutation $\widehat{T}$ can be thought of as the shift on $\mathcal{B}^{\mathbb{Z}}$.

We observe that full-length sequences based on the discretized Markov transformation are nothing but in $\mathcal{L}_{|\mathcal{B}|}(X_{A_H})$, which implies the discretized Markov transformation $\widehat{T} : \mathcal{Q} \to \mathcal{Q}$ is only one step of the approximation of the underlying transformation $T : [0, 1] \to [0, 1]$. In order to define more refined approximations, we introduce the notion of higher edge graph from symbolic dynamics [7].

Definition 3 *Let G be a graph. For $n \geq 2$ we define the nth higher edge graph $G^{[n]}$ of G to have vertex set $\mathcal{L}_{n-1}(X_{A_G})$ and to have edge set containing exactly one edge from $e_1e_2 \cdots e_{n-1}$ to $f_1f_2 \cdots f_{n-1}$ whenever $e_2e_3 \cdots e_{n-1} = f_1f_2 \cdots f_{n-2}$ (or $\mathbf{t}(e_1) = \mathbf{i}(f_1)$ if $n = 2$), and none otherwise. The edge is named $e_1e_2e_3 \cdots e_{n-1}f_{n-1} = e_1f_1f_2 \cdots f_{n-1}$. For $n = 1$ we set $G^{[1]} = G$.*

Let G be the graph representing the Markov transformation. Then we obtain a sequence $(G^{[n]})_{n=1}^{\infty}$ of higher edge graphs of G. For each $n \geq 1$, we use $H_n = (\mathcal{L}_{n-1}(X_{A_G}), \mathcal{B}_n)$ to denote the Eulerian subgraph spanning $G^{[n]}$ with maximal number of edges, each of which leads to a discretized Markov transformation $\widehat{T}_n$. Recall that the length is given by $|\mathcal{B}_n|$.

Example 1 *Let $T : [0, 1] \to [0, 1]$ be the dyadic transformation: $T(x) = 2x \ (mod\ 1)$, $x \in [0, 1]$. If we take a Markov partition of $[0, 1]$ given by the point $0 < 1/2 < 1$, then we obtain the graph G representing the dyadic transformation as shown in Fig. 1.*

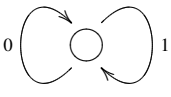

Figure 1: $G = G^{[1]} = H_1$.

For each n (≥ 1), we obtain $G^{[n]} = (\{0, 1\}^{n-1}, \{0, 1\}^n)$, which is called the de Bruijn graph. Since $G^{[n]}$ is Eulerian, we have $H_n = G^{[n]}$ for each n. The Eulerian circuits in $G^{[n]}$ are called the de Bruijn sequences of length 2^n.

4. Correlational Properties of the de Bruijn Sequences

The correlation functions for sequences are measures of the similarity, or relatedness, between two sequences. Mathematically they are defined as follows.

Definition 4 *The cross-correlation function of time delay ℓ for the sequences $\boldsymbol{X} = (X_i)_{i=0}^{N-1}$ and $\boldsymbol{Y} = (Y_i)_{i=0}^{N-1}$ over $\{-1, 1\}$ is defined by*

$$R_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = \sum_{i=0}^{N-1} X_i Y_{i+\ell \,(\mathrm{mod}\, N)},$$

where $\ell = 0, 1, \cdots, N-1$ and, for integers a and $b\,(\geq 1)$, $a\,(\mathrm{mod}\ b)$ denotes the least residue of a to modulus b. The normalized cross-correlation function of time delay ℓ for the sequences $\boldsymbol{X}$ and $\boldsymbol{Y}$ is defined by

$$r_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = \frac{1}{N} \sum_{i=0}^{N-1} X_i Y_{i+\ell \,(\mathrm{mod}\, N)}.$$

If $\boldsymbol{X} = \boldsymbol{Y}$, we call $R_N(\ell; \boldsymbol{X}, \boldsymbol{X})$ and $r_N(\ell; \boldsymbol{X}, \boldsymbol{X})$ the auto-correlation function and the normalized auto-correlation function, and simply denote them by $R_N(\ell; \boldsymbol{X})$ and $r_N(\ell; \boldsymbol{X})$, respectively.

In this study, we are concerned with correlational properties of the de Bruijn sequences and the full-length sequences based on the discretized golden mean transformation. As we see above, a de Bruijn sequence is usually defined as a sequence over $\{0, 1\}$ while the correlation functions are defined for a sequence over $\{-1, 1\}$. Throughout this report, when we compute the values of the normalized cross-correlation functions $r_N(\ell; \boldsymbol{X}, \boldsymbol{Y})$ for the sequences $\boldsymbol{X}$ and $\boldsymbol{Y}$ over $\{0, 1\}$, we regard 0 in the sequences over $\{0, 1\}$ as -1. In other words, we transform the sequences $\boldsymbol{X}$ and $\boldsymbol{Y}$ of length N over $\{0, 1\}$ to sequences of length N over $\{-1, 1\}$ by one-to-one correspondence between 0 and -1, respectively.

By the definition, we immediately see the following.

Remark 1 *For any $\boldsymbol{X}$, we have*

$$r_N(0; \boldsymbol{X}) = 1.$$

The following basic properties of the normalized auto-correlation functions for the de Bruijn sequences are well known [5].

Theorem 1 *Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be the de Bruijn sequences of length $N = 2^n$ $(n \geq 1)$. Then we have*

i) $$\sum_{\ell=0}^{N-1} r_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = 0;$$

ii) $$r_N(\ell; \boldsymbol{X}) = 0 \quad \textit{for} \quad 1 \leq \ell \leq n-1.$$

5. Correlational Properties of the the Full-Length Sequences Based on the Discretized Golden Mean Transformation

Let $T : [0, 1] \to [0, 1]$ be the golden mean transformation: $T(x) = \beta x \pmod 1$, $x \in [0, 1]$, where β is the golden mean number $\frac{1+\sqrt{5}}{2}$. The graph of T is given in Fig. 2.

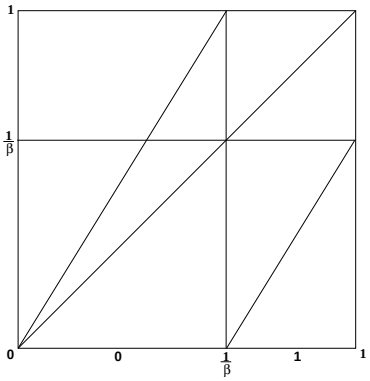

Figure 2: The golden mean transformation.

If we take a Markov partition of $[0, 1]$ given by the point $0 < 1/\beta^2 < 1/\beta < 1$, then we obtain the graph G representing the golden mean transformation as shown in Fig. 3.

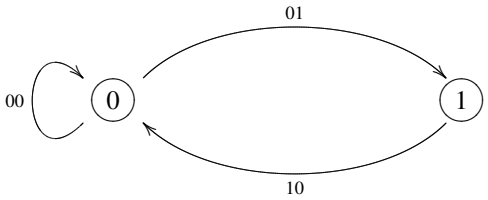

Figure 3: $G^{[2]} = H_2$.

In view of $G^{[2]}$ in Fig. 3, the set of forbidden blocks is given by $\mathcal{F} = \{11\}$. For each n (≥ 2), we obtain $G^{[n]} = (\mathcal{L}_{n-1}(X_{\mathcal{F}}), \mathcal{L}_n(X_{\mathcal{F}}))$ and the Eulerian subgraph $H_n = (\mathcal{L}_{n-1}(X_{\mathcal{F}}), \mathcal{B}_n)$ spanning $G^{[n]}$ with maximal number of edges. Although $G^{[2]}$ is Eulerian, which implies $H_2 = G^{[2]}$, $G^{[n]}$ is not always Eulerian for n (≥ 3). In fact, H_3 is a proper subgraph of $G^{[3]}$, in symbols $H_3 \subsetneqq G^{[3]}$. We observed in [3] that $H_n \subsetneqq G^{[n]}$ for any n (≥ 3).

Noting that the sequence $(|\mathcal{B}_n|)_{n=2}^{\infty}$ is the Fibonacci numbers defined by the recurrence relation $|\mathcal{B}_n| = |\mathcal{B}_{n-1}| + |\mathcal{B}_{n-2}|$ (≥ 4) with $|\mathcal{B}_2| = 3$ and $|\mathcal{B}_3| = 4$, we obtain

$$|\mathcal{B}_n| = \beta^n + \overline{\beta}^n \quad \text{for} \quad n \geq 2, \tag{1}$$

where $\overline{\beta} = \frac{1-\sqrt{5}}{2}$.

In virtue of symbolic analysis of $\mathcal{L}_n(X_{\mathcal{F}})$ and $\mathcal{B}_n$, we obtain

Theorem 2 *Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be full-length sequences based on the discretized golden mean transformation of length $|\mathcal{B}_n|$.*

Then we obtain

$$\sum_{\ell=0}^{|\mathcal{B}_n|-1} r_{|\mathcal{B}_n|}(\ell;\boldsymbol{X},\boldsymbol{Y}) = \frac{(\beta^n-\overline{\beta}^n)^2}{\left\{(\beta^n-\overline{\beta}^n)+2(\beta^{n-1}-\overline{\beta}^{n-1})\right\}^2}.$$

Asymptotically, we obtain

Remark 2

$$\lim_{n\to\infty}\sum_{\ell=0}^{|\mathcal{B}_n|-1} r_{|\mathcal{B}_n|}(\ell;\boldsymbol{X},\boldsymbol{Y}) = \frac{\beta^2}{(\beta+2)^2}.$$

Moreover, we obtain

Theorem 3 *Let $\boldsymbol{X}$ be a full-length sequence based on the discretized golden mean transformation of length $|\mathcal{B}_n|$. Then for $1 \le \ell \le n-1$, we obtain*

$$r_{|\mathcal{B}_n|}(\ell;\boldsymbol{X}) = \frac{1}{(\beta-\overline{\beta})^2}\left(1+4(-1)^\ell\frac{\beta^{n-2\ell}+\overline{\beta}^{n-2\ell}}{\beta^n+\overline{\beta}^n}\right).$$

On the other hand, for the stationary Markov process $(Z_n)_{n=0}^{\infty}$ over $\{-1,1\}$ with the transition matrix $\begin{pmatrix} \frac{1}{\beta} & \frac{1}{\beta^2} \\ 1 & 0 \end{pmatrix}$, we obtain

$$\mathbb{E}[Z_nZ_{n+\ell}] = \frac{1}{(\beta-\overline{\beta})^2}\left(1+4(-1)^\ell\beta^{-2\ell}\right) \quad \text{for} \quad \ell \ge 0. \quad (2)$$

For a random variable X, we use $\mathbb{E}[X]$ to denote the expected value of X.

Now let us estimate the error of the normalized autocorrelation function, which is originated from the discretization of the underlying transformations. In view of Theorem 3, (2) leads to

Observation 1

$$r_{|\mathcal{B}_n|}(\ell;\boldsymbol{X}) - \mathbb{E}[Z_nZ_{n+\ell}] = \frac{4(-1)^\ell}{(\beta-\overline{\beta})^2}\cdot\frac{\left(\frac{\overline{\beta}}{\beta}\right)^n}{1+\left(\frac{\overline{\beta}}{\beta}\right)^n}\cdot(\beta^{2\ell}-\overline{\beta}^{2\ell}) \quad (3)$$

and

$$\lim_{n\to\infty} r_{|\mathcal{B}_n|}(\ell;\boldsymbol{X}) = \mathbb{E}[Z_nZ_{n+\ell}].$$

The equation (3) implies

$$r_{|\mathcal{B}_n|}(\ell;\boldsymbol{X}) = \mathbb{E}[Z_nZ_{n+\ell}] + O\left(\left(\frac{\overline{\beta}}{\beta}\right)^n\right), \quad (4)$$

where O is the big O notation from the Landau symbol. The error $O\left(\left(\frac{\overline{\beta}}{\beta}\right)^n\right)$ can be regarded as coming from the discretization of the underlying β transformation. It is noteworthy that (4) holds even for the de Bruijn sequences in the following sense. If the underlying transformation is the dyadic transformation, we have $\beta = 2$ and $\overline{\beta} = 0$. Thus we obtain $O\left(\left(\frac{\overline{\beta}}{\beta}\right)^n\right) = 0$ for the de Bruijn sequences. In view of Theorem 1 ii) together with this fact, (4) holds for the de Bruijn sequences if $(Z_n)_{n=0}^{\infty}$ is a sequence of independent and identically distributed (i.i.d.) random variables over $\{-1,1\}$ with uniform distributions.

6. Summary

We considered the discretized golden mean transformation. In view of basic properties of the normalized autocorrelation functions for the de Bruijn sequences that can be regarded as the full-length sequences based on the discretized dyadic transformation, we obtained correlational properties of the full-length sequences based on the discretized golden mean transformation.

References

[1] 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).

[2] 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, pp.1327–1332, 2002.

[3] H. Fujisaki, "Discretized Markov Transformations – An Example of Ultradiscrete Dynamical Systems –," *IEICE Trans. Fundamentals*, vol. E88-A, pp.2684–2691, 2005.

[4] H. Fujisaki, "An Algorithm For Generating All Full-Length Sequences Which Are Based On Discretized Markov Transformations," *NOLTA, IEICE*, vol. 1, pp. 166–175, 2010.

[5] Z. Zhang and W. Chen, "Correlation properties of de Bruijn sequences," *Systems Science and Mathematical Sciences*, vol. 2, pp. 170–183, 1989.

[6] H. Fujisaki and Y. Nabeshima, "On Auto-Correlation Values of de Bruijn Sequences," *NOLTA, IEICE*, vol. 3, pp. 400–408, 2011.

[7] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge Univ. Press, 1995.

[8] B. Kitchens, *Symbolic dynamics: One-sided, two-sided, and countable state Markov shifts*, Springer, 1998.

[9] H. Fredricksen, "A Survey of Full Length Nonlinear Shift Register Cycle Algorithm," *SIAM Review*, vol. 24, pp. 195–221, 1982.

[10] H. Fujisaki, "A construction of all CR sequences in the de Bruijn sequences of length 2^{2p+1} where p is a prime number," *NOLTA, IEICE*, vol. 5, pp. 235–249, 2014.

[11] H. Fujisaki, "An algorithm for generating all CR sequences in the de Bruijn sequences of length 2^n where n is any odd number," *NOLTA, IEICE*, vol. 6, pp. 329–339, 2015.