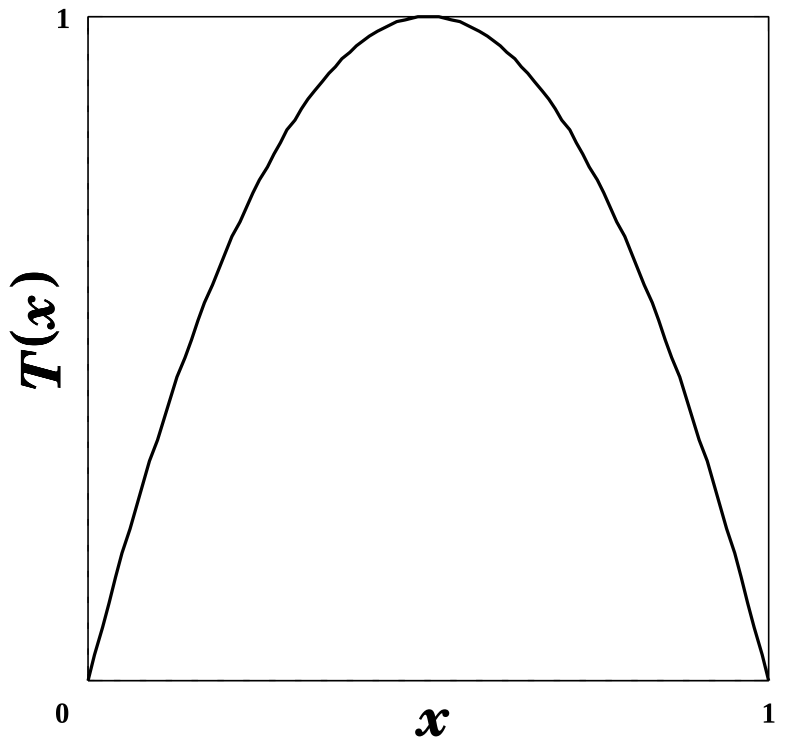
The topological entropy and correlational properties of the discretized Markov β-transformations and their applications

Hiroshi FUJISAKI

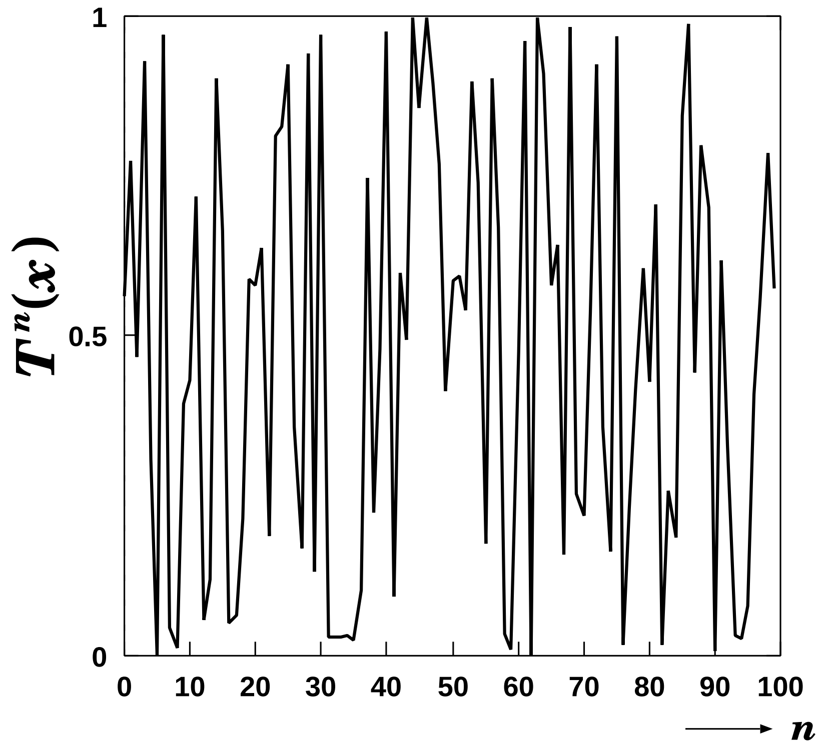
Kanazawa University

Jan. 31, 2017

- Ulam and von Neumann (Bull. Math. Soc., 1947)
  Logistic map: $T(x) = 4x(1-x)$, $0 \le x \le 1$



$\Rightarrow$



Given an initial value $x = T^0(x)$,

$$T^n(x) = T(T^{n-1}(x)) \quad \text{for} \quad n = 1, 2, \cdots .$$

The sequence $(T^n(x))_{n=0}^{\infty}$ is a good candidate for the *pseudo-random numbers*.

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.

> No way is known to give a good theoretical model that tells us characteristics of the execution time for *floating point numbers*. (D. Knuth, *The Art of Computer Programming*, vol. 2, 3rd ed., Addison-Wesley, '97)

Discretized Bernoulli Transformations

○ Cryptosystems

- Permutation Cipher Based on Discretized Unimodal Bernoulli Transformations (N. Masuda and K. Aihara, *Trans. of IEICE*, '99 (in Japanese))

○ Spreading Seq.s for SSMA Communication Systems

- Maximal-Period Sequences Based on Discretized Bernoulli Transformations (A. Tsuneda, Y. Kuga, and T. Inoue, *IEICE Trans. on Funda.*, 2002)

A Generalization of *de Bruijn Sequences*

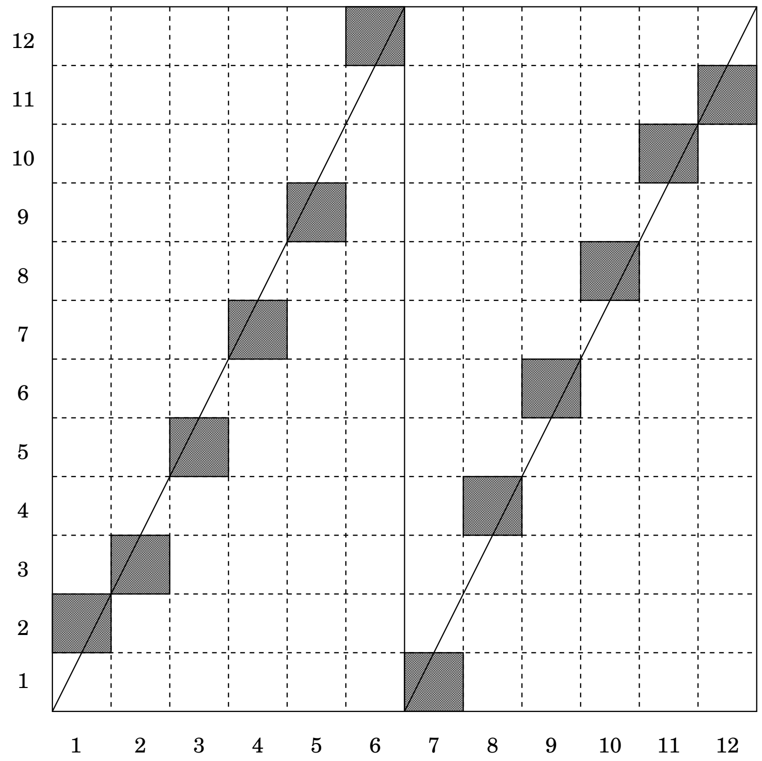
Markov Partition

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

Definition 1 *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 the interior of some connected union of the closures 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*.*

An example of discretized dyadic transformations ($2m = 12$):

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

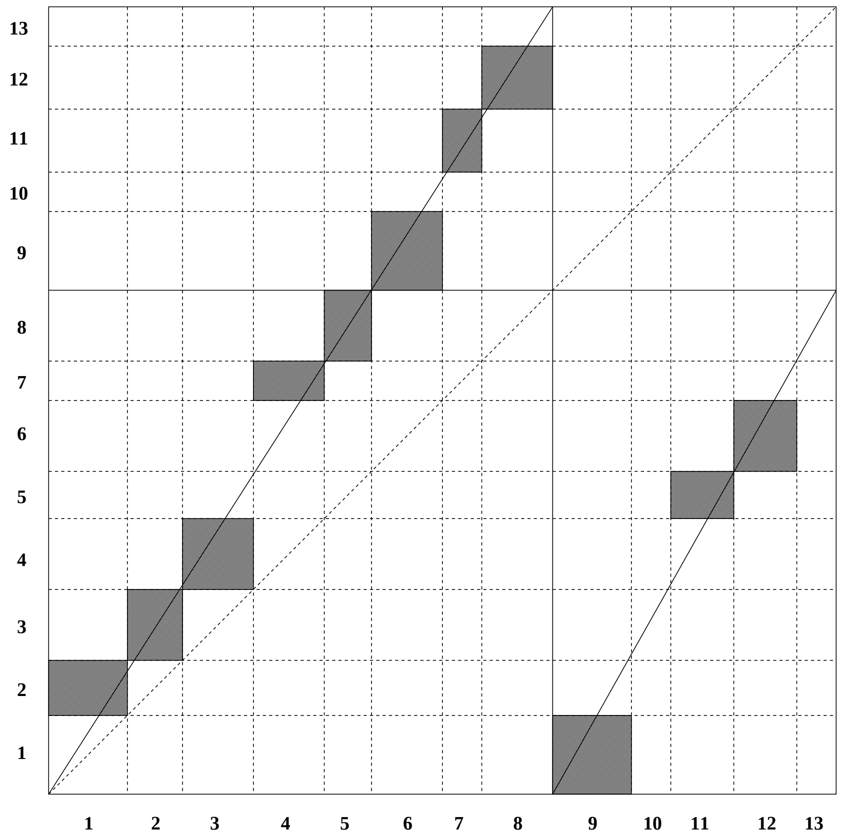


σ determines a full-length sequence 000010111101.
If $2m = 2^n$, then the full-length sequence is called the de Bruijn sequence.

Discretized Golden Mean Transformations

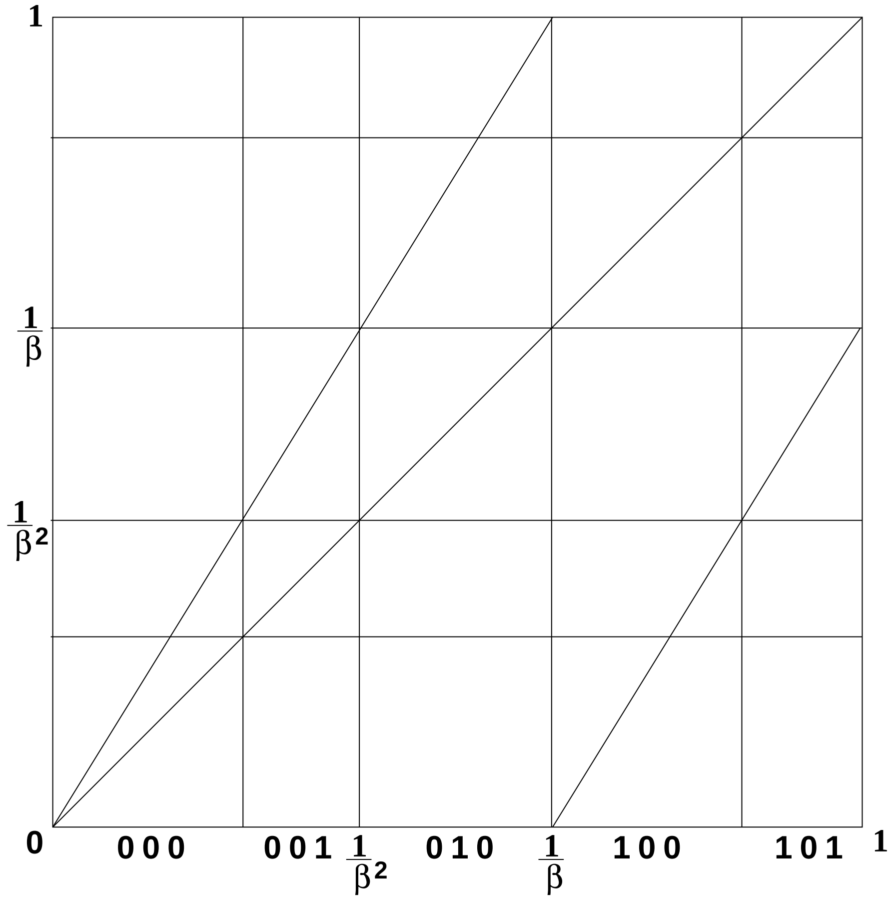
$$\sigma = \begin{pmatrix} I_1 & I_2 & I_3 & I_4 & I_5 & I_6 & I_7 & I_8 & I_9 & I_{11} & I_{12} \\ I_2 & I_3 & I_4 & I_7 & I_8 & I_9 & I_{11} & I_{12} & I_1 & I_5 & I_6 \end{pmatrix}.$$

Note that I_{10} and I_{13} are excluded from the Markov partion.



σ determines a full-length sequence 00000100101. [F. Enomoto and S. Ito, Workshop Number Theory and Ergodic Theory, 2004)]

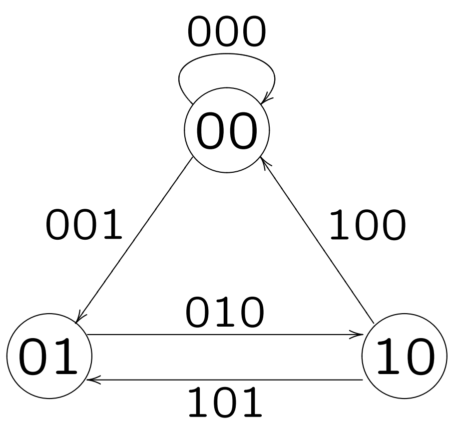
Graph Represention of the Markov Transformation

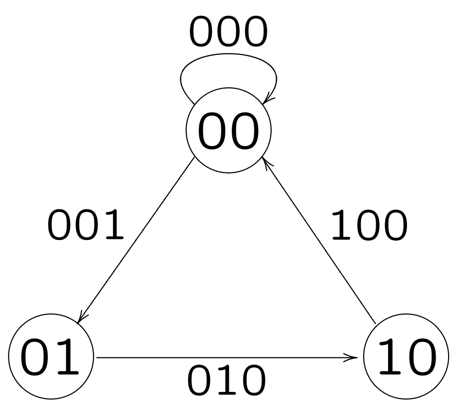


For an irreducible aperiodic Markov transformation T, given a Markov partition $\mathcal{P}$ with respect to T, corresponding each subinterval $I \in \mathcal{P}$ to one edge $e(I)$, we obtain the set $\mathcal{A}$ of edges.

Eulerian Subgraph Spanning G

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 edges.





The spanning Eulerian subgraph with maximal number of edges

Full-length sequences based on the discretized Markov transformation are exactly Eulerian circuits in H, whose length is given by $|\mathcal{B}|$.

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 $u = u_1 u_2 \cdots u_n \in \Sigma^n$ 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 $\mathcal{L}_0(X) = \{\epsilon\}$.

Definition 2 *The topological entropy of a subshift X is defined by*

$$h(X) = \lim_{n \to \infty} \frac{1}{n} \log |\mathcal{L}_n(X)|.$$

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

Higher Edge Graph

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 $e_1 e_2 \cdots e_{n-1}$ to $f_1 f_2 \cdots f_{n-1}$ whenever $e_2 e_3 \cdots e_{n-1} = f_1 f_2 \cdots f_{n-2}$ (or $\mathbf{t}(e_1) = \mathbf{i}(f_1)$ if $n = 2$), and none otherwise. The edge is named*

$$e_1 e_2 e_3 \cdots e_{n-1} f_{n-1} = e_1 f_1 f_2 \cdots f_{n-1}.$$

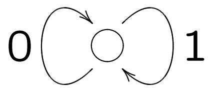
For $n = 1$ we set $G^{[1]} = G$.

Discretized Dyadic Transformations

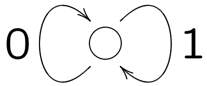
Let $T : [0,1] \to [0,1]$ be the dyadic transformation:

$$T(x) = 2x \ (\mathrm{mod}\ 1), \ x \in [0,1].$$

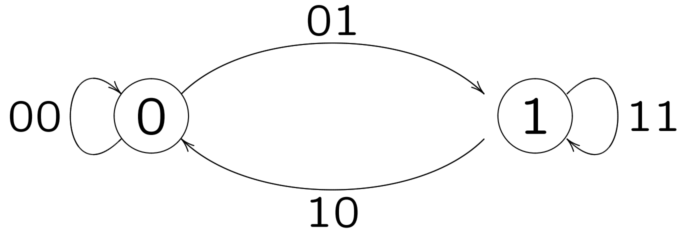
If we take a Markov partition of $[0,1]$ given by the point $0 < 1/2 < 1$, then we obtain the graph G representing the dyadic transformation.



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



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



$G^{[2]} = H_2.$

For each n (≥ 1), we obtain $G^{[n]} = (\{0,1\}^{n-1}, \{0,1\}^n)$. 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 because of the following theorem. For the same reason, $G^{[n]}$ is called the de Bruijn graph.

Theorem 1 (de Bruijn, 1946, Flye Sainte-Marie, 1894) *For each positive integer n, there are exactly $2^{2^{n-1}-n}$ Eulerian circuits in $G^{[n]}$.*

The Topological Entropy of Discretized Markov Transformation

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 $\widehat{T}_n$.

We use ν_n to denote the number of the full-length sequence in H_n. Recall that the length is given by $|\mathcal{B}_n|$.

Definition 4 *The topological entropy of the discretized Markov transformation $\mathcal{T} = (\widehat{T}_n)_{n=1}^{\infty}$ of T is defined by*

$$h_{\mathcal{T}} = \lim_{n \to \infty} \frac{1}{|\mathcal{B}_n|} \log \nu_n.$$

Example 1 *The topological entropy of the discretized dyadic transformation* $\mathcal{T}$ *is given by*

$$h_{\mathcal{T}} = \frac{1}{2}\log 2.$$

Remark 1 *Since it is also shown in [de Bruijn, 1946] and [Flye Sainte-Marie, 1894] that, for each* n (≥ 1), *there are exactly*

$$\{(k-1)!\}^{k^{n-1}} k^{k^{n-1}-n}$$

Eulerian circuits of length k^n *in*

$$G^{[n]} = (\{0, 1, \cdots, k-1\}^{n-1}, \{0, 1, \cdots, k-1\}^n),$$

the topological entropy of the discretized k*-adic transformation is given by*

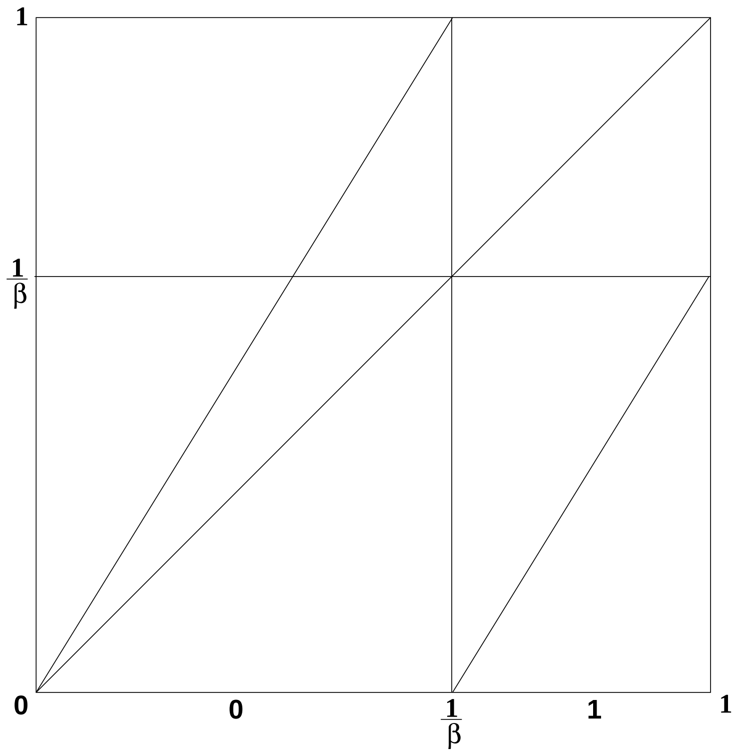
$$\frac{1}{k}\log(k!).$$

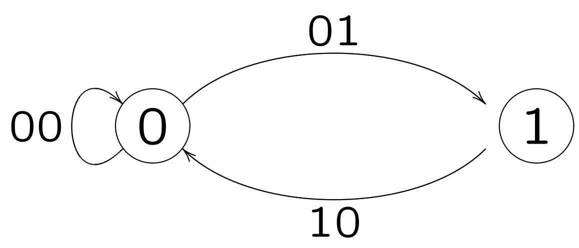
Discretized Golden Mean Transformation

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 $\frac{1+\sqrt{5}}{2}$.





$$G^{[2]} = H_2.$$

In view of $G^{[2]}$, 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 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 $\overline{\beta} = \frac{1-\sqrt{5}}{2}$.

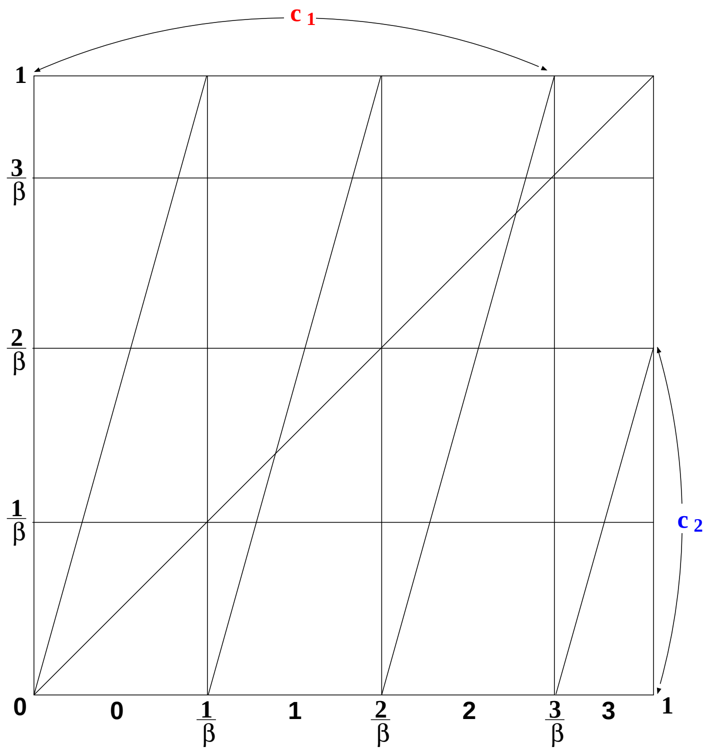
The topological entropy of the discretized golden mean transformation is given by

Theorem 2

$$\lim_{n\to\infty} \frac{1}{|\mathcal{B}_n|} \log \nu_n = \frac{1}{\beta(\beta - \overline{\beta})} \log 2.$$

A Class of Markov Transformations Associated with Greedy β-Expansion

Now we are in the position to consider the discretized Markov β-transformations with the alphabet $\Sigma = \{0, 1, \cdots, k-1\}$ $(k \geq 2)$ and the set $\mathcal{F} = \{(k-1)c, \cdots, (k-1)(k-1)\}$ $(1 \leq c \leq k-1)$ of $(k-c)$ forbidden blocks. Setting $c_1 = k-1$ and $c = c_2$, β is the positive solution of $t^2 - c_1 t - c_2 = 0$.



Generally we have

Theorem 3

$$\lim_{n\to\infty} \frac{1}{|\mathcal{B}_n|} \log \nu_n = \frac{c_2}{\beta(\beta - \overline{\beta})} \log(k!) + \frac{\beta - c_2}{\beta(\beta - \overline{\beta})} \log\{(k-1)!\} + \frac{1}{\beta(\beta - \overline{\beta})} \log(c_2!).$$

Variational Principle

Definition 5 *If λ is the Perron-Frobenius eigenvalue of A and $(u_0, \cdots, u_{|\Sigma|-1})$ is a strictly positive left eigenvector and $(v_0, \cdots, v_{|\Sigma|-1})$ is a strictly positive right eigenvector with $\sum_{i=0}^{|\Sigma|-1} u_i v_i = 1$, then we obtain a Markov measure given by a probability vector $p = (p_0, \cdots, p_{|\Sigma|-1})$ and a stochastic matrix $P = (p_{i,j})$ where*

$$p_i = u_i v_i \quad \text{and} \quad p_{i,j} = \frac{a_{i,j} v_j}{\lambda v_i}.$$

We call this measure the Parry measure for $\sigma : X_A \to X_A$.

We obtain

$$-\sum_{i,j} p_i p_{i,j} \log p_{i,j} = \log \lambda.$$

The left hand side is the Shannon entropy for a Markov chain given by (p, P) while the right hand side is the topological entropy of $\sigma : X_A \to X_A$.

Correlational Properties of the de Bruijn Sequences

Definition 6 *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 $\Sigma = \{0, 1, \cdots, k-1\}$ $(k \geq 2)$ is defined by*

$$R_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = \sum_{i=0}^{N-1} \exp\left(\frac{X_i}{k} 2\pi\sqrt{-1}\right) \exp\left(-\frac{Y_{i+\ell \pmod N}}{k} 2\pi\sqrt{-1}\right),$$

where $\ell = 0, 1, \cdots, N-1$ and, for integers a and $b\,(\geq 1)$, $a \pmod b$ 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

$$r_N(\ell; \boldsymbol{X}, \boldsymbol{Y}) = \frac{1}{N} R_N(\ell; \boldsymbol{X}, \boldsymbol{Y}).$$

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.

By the definition, we immediately see the following.

Remark 2 *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 [Zhang & Chen, 1989].

Theorem 4 *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) $$r_N(\ell; \boldsymbol{X}) = 0 \quad \text{for} \quad 1 \leq \ell \leq n-1.$$

(Zero Correlation Zone (ZCZ))

Observation 1 *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, Theorem 4 ii) implies*

$$r_N(\ell; \boldsymbol{X}) = \mathbb{E}[Z_0 Z_\ell] \quad \text{for} \quad 0 \leq \ell \leq n-1.$$

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

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

Theorem 5 *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*

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

Asymptotically, we obtain

Remark 3

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

Moreover, we obtain

Theorem 6 *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*

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

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

$$\mathbb{E}[Z_0 Z_\ell] = \frac{1}{(\beta-\overline{\beta})^2}\left\{1+4\left(\frac{\overline{\beta}}{\beta}\right)^{\ell}\right\} \quad \text{for} \quad \ell \geq 0. \tag{2}$$

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

Discussions

Now let us estimate the error of the normalized auto-correlation function, which is originated from the discretization of the underlying transformations. In view of Theorem 6, (2) leads to

Observation 2

$$r_{|\mathcal{B}_n|}(\ell; \boldsymbol{X}) - \mathbb{E}[Z_0 Z_\ell] = \left\{ \left(\frac{\beta}{\overline{\beta}}\right)^{\ell} - \left(\frac{\overline{\beta}}{\beta}\right)^{\ell} \right\} \cdot \frac{\left(\frac{\overline{\beta}}{\beta}\right)^{n}}{1 + \left(\frac{\overline{\beta}}{\beta}\right)^{n}} \tag{3}$$

and

$$\lim_{n \to \infty} r_{|\mathcal{B}_n|}(\ell; \boldsymbol{X}) = \mathbb{E}[Z_0 Z_\ell].$$

The equation (3) implies

$$r_{|\mathcal{B}_n|}(\ell; \boldsymbol{X}) = \mathbb{E}[Z_0 Z_\ell] + O\left(\left(\frac{\overline{\beta}}{\beta}\right)^n\right), \tag{4}$$

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.

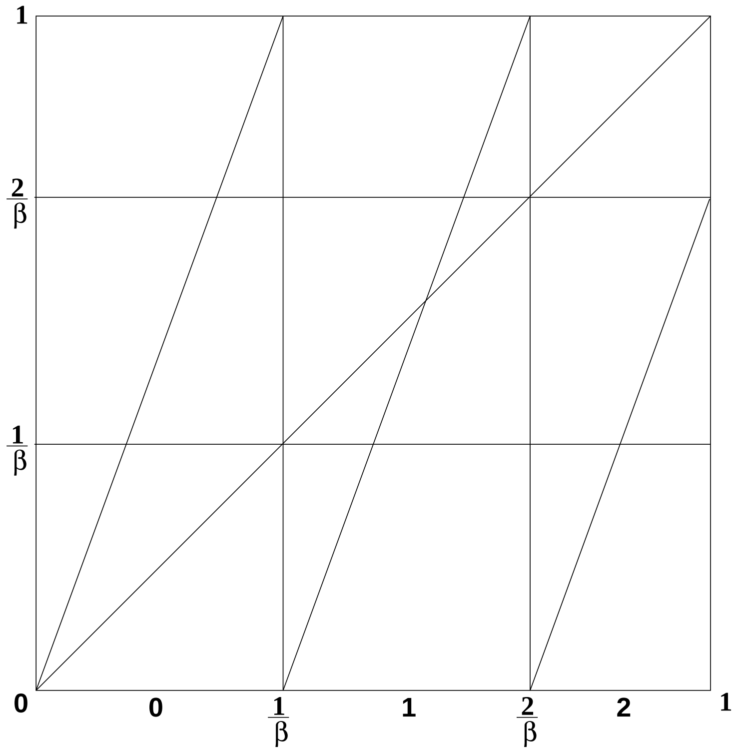
It is noteworthy that (4) holds even for the de Bruijn sequences in the following sense. If the underlying transformation is the dyadic transformation, we have $\beta = 2$ and $\overline{\beta} = 0$. Thus we obtain $O\left(\left(\frac{\overline{\beta}}{\beta}\right)^{2^n}\right) = 0$ for the de Bruijn sequences.

In view of Theorem 4 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.

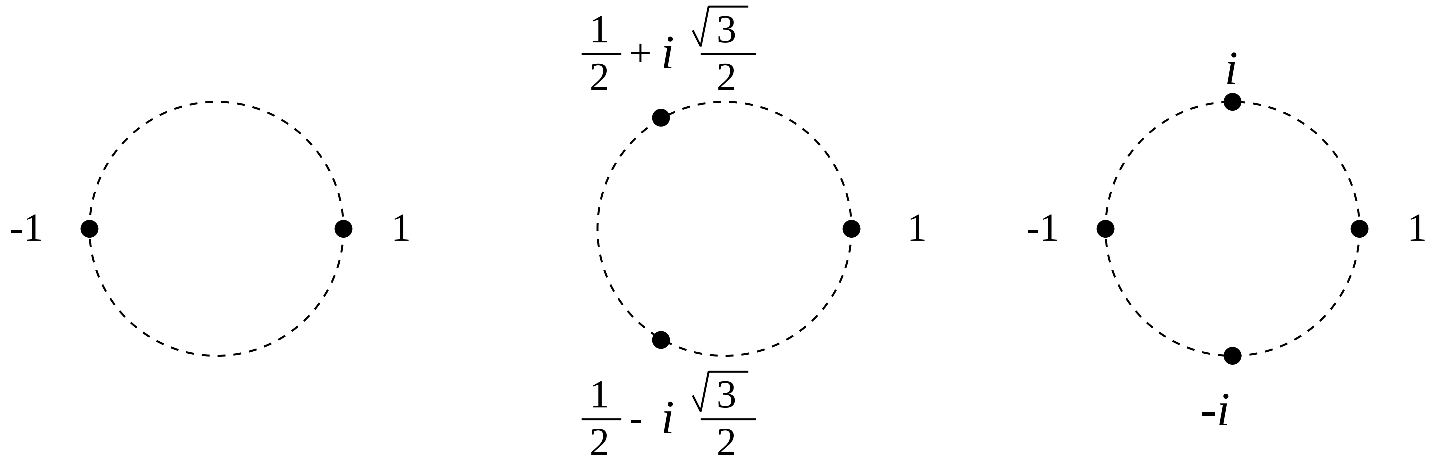
Full-Length Sequences Based on the Discretized Markov β-Transformations

We consider the discretized Markov β-transformations with the alphabet $\Sigma = \{0, 1, \cdots, k-1\}$ and the set $\mathcal{F} = \{(k-1)(k-1)\}$ of forbidden blocks ($k \geq 2$).

For $\Sigma = \{0, 1, 2\}$ and $\mathcal{F} = \{22\}$, as the underlying transformation, we have the β-transformation with $\beta = 1 + \sqrt{3}$.



k-Phase Signals



Binary 3-Phase Q-Phase

$$\mathbb{E}[Z_0 Z_\ell] = \frac{1}{(k-1)^2(\beta - \overline{\beta})^2}\left(\left\{\beta + (k-1)\overline{\beta}\right\} + (k-1)k^2\left(\frac{\overline{\beta}}{\beta}\right)^\ell\right)$$

for $\quad \ell \geq 0.$

By using exactly the same manner as above, we generally obtain

Theorem 7

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

Asymptotically, we obtain

Remark 4

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

Moreover, we obtain

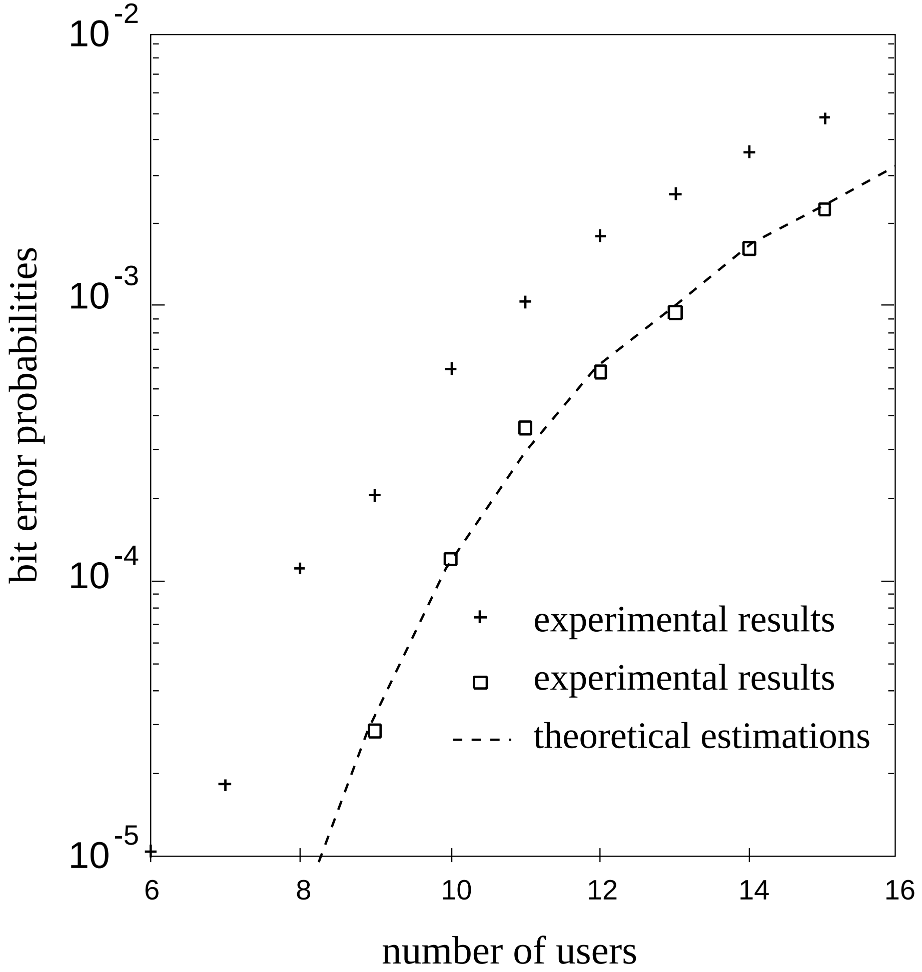
Theorem 8 *Let $\boldsymbol{X}$ be a full-length sequence based on the discretized Markov β-transformation of length $|\mathcal{B}_n|$ with with the alphabet $\Sigma = \{0, 1, \cdots, k-1\}$ and the set $\mathcal{F} = \{(k-1)(k-1)\}$ of forbidden blocks. Then for $1 \le \ell \le n-1$, we obtain*

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

This implies

$$r_{|\mathcal{B}_n|}(\ell; \boldsymbol{X}) = \mathbb{E}[Z_0 Z_\ell] + O\left(\left(\frac{\overline{\beta}}{\beta} \right)^{n} \right).$$

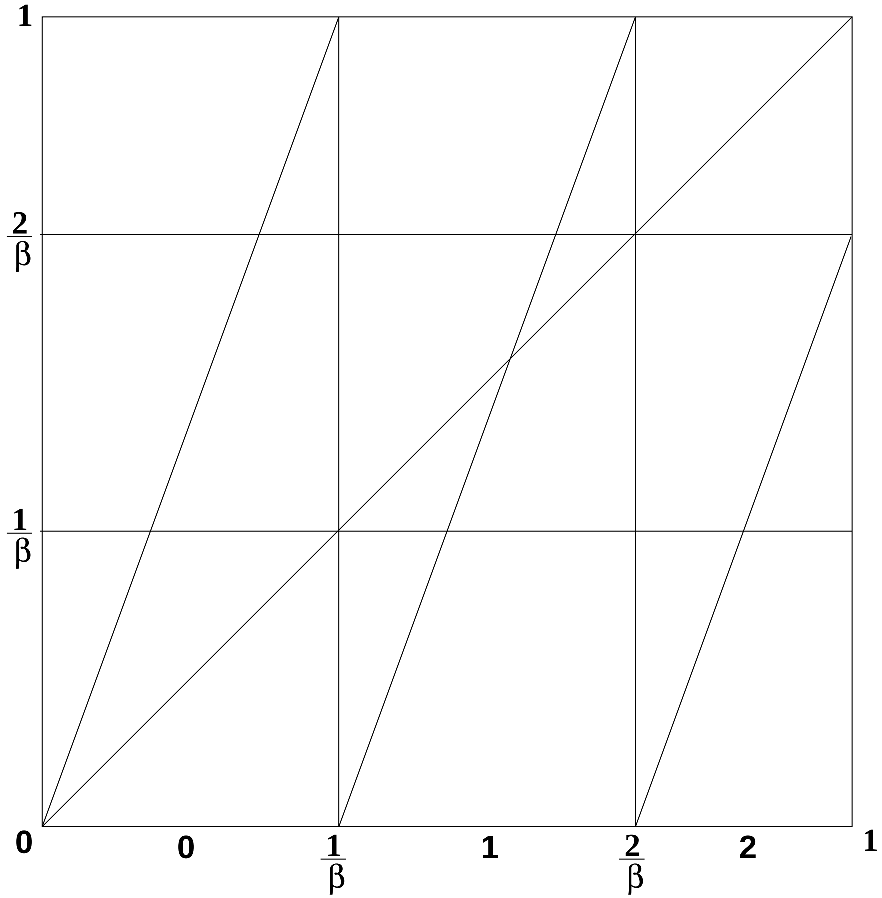
Optimum Binary Spreading Sequences of Markov Chains



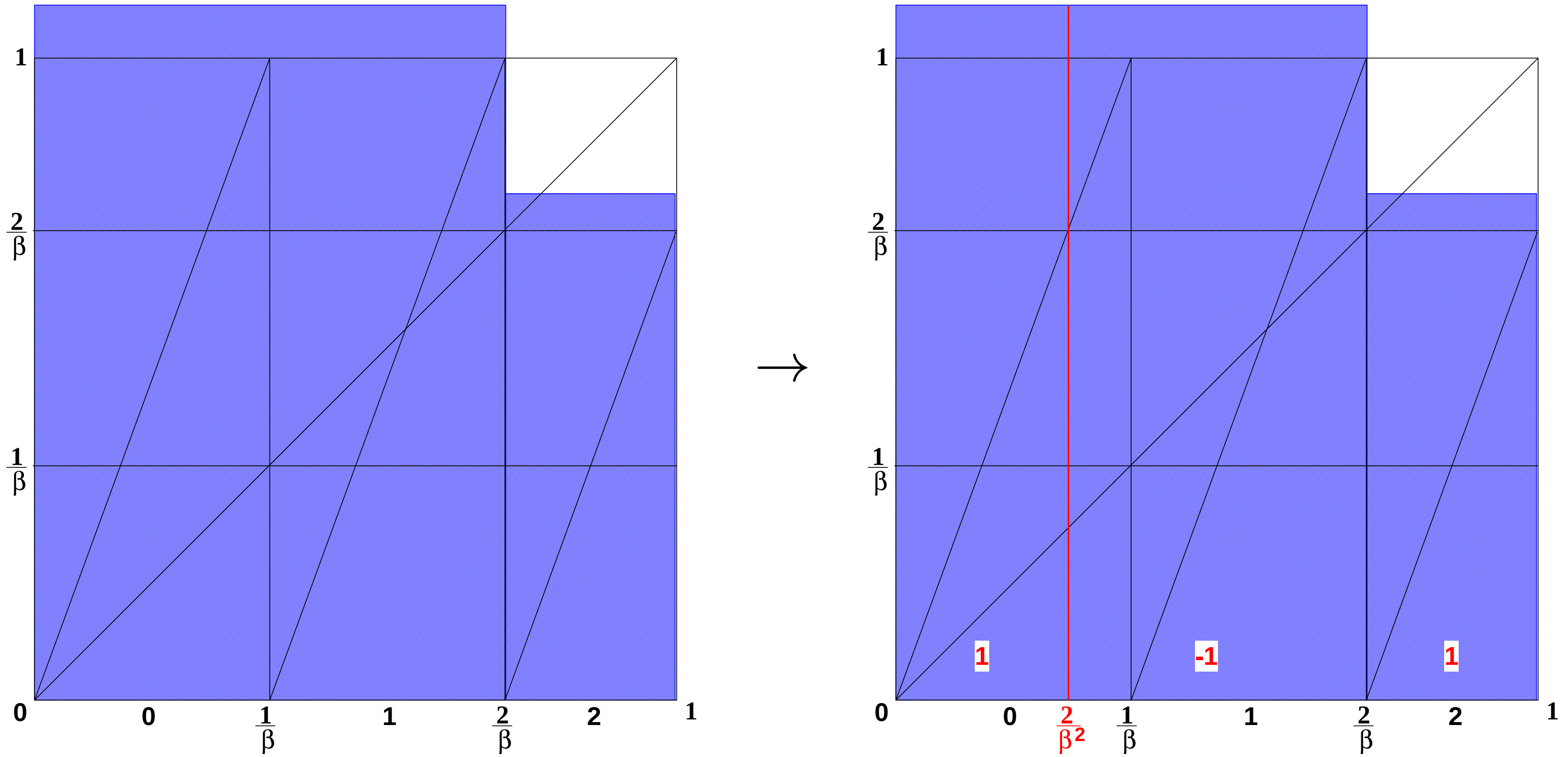
$\{1, -1\}$-valued Markov chains with

$$\mathbb{E}[Z_n] = 0 \quad \text{and} \quad \mathbb{E}[Z_0 Z_\ell] = (-2+\sqrt{3})^\ell, \quad \ell \geq 0.$$

We consider the Markov β-transformations with the alphabet $\Sigma = \{0, 1, 2\}$ and the set $\mathcal{F} = \{22\}$ of forbidden blocks. Then we have the β-transformation with $\beta = 1 + \sqrt{3}$.



Design of Simple Functions



$$\Theta(x) = \mathbf{1}_{[0,\frac{2}{\beta^2})}(x) - \mathbf{1}_{[,\frac{2}{\beta^2},\frac{2}{\beta})}(x) + \mathbf{1}_{[\frac{2}{\beta},1]}(x).$$

$$\mathbb{E}[Z_n] = 0, \ \text{(uniform distribution)}$$

and

$$\mathbb{E}[Z_0 Z_\ell] = (-2+\sqrt{3})^\ell, \quad \ell \geq 0, \ \text{negative correlation as desired!}$$

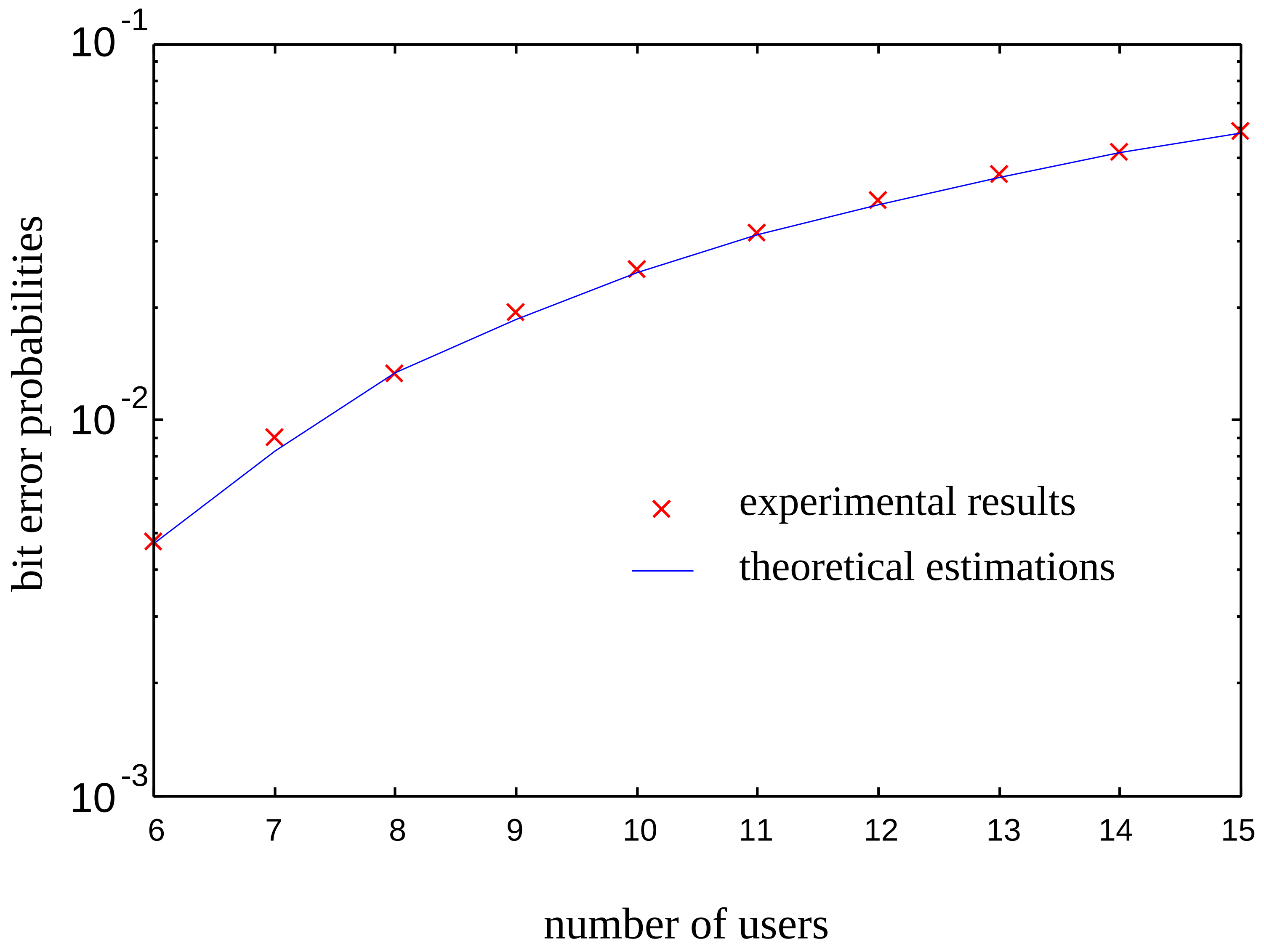
Experimental Results

n	length	# of seq.s	# of seq.s w/ uniform dist.
2	8	12	6
3	20	1728	945

Example 2 *For the order* $n = 3$*, we have*

$$00010020110121021112 \rightarrow 11101011001010010001,$$

where in the right hand side, we use 0 *to denote* -1 *for simplicity.*



10^-1
10^-2
10^-3
bit error probabilities
6
7
8
9
10
11
12
13
14
15
number of users
experimental results
theoretical estimations

Theorem 9 *For $1 \leq \ell \leq n-1$, we obtain*

$$r_{|\mathcal{B}_n|}(\ell; \boldsymbol{X}) = (-2+\sqrt{3})^{\ell} + \left\{ \left(\frac{\beta}{\overline{\beta}}\right)^{\ell} - \left(\frac{\overline{\beta}}{\beta}\right)^{\ell} \right\} \cdot \frac{\left(\frac{\overline{\beta}}{\beta}\right)^{n}}{1 + \left(\frac{\overline{\beta}}{\beta}\right)^{n}} \, .$$

This implies

$$r_{|\mathcal{B}_n|}(\ell; \boldsymbol{X}) = \mathbb{E}[Z_0 Z_\ell] + O\left(\left(\frac{\overline{\beta}}{\beta}\right)^{n} \right).$$

Summary

In this reserch, we first obtained the topological entropy of the discretized golden mean transformation. We also generalized this result and gave the topological entropy of the discretized Markov β-transformations with the alphabet $\Sigma = \{0, 1, \cdots, k-1\}$ and the set $\mathcal{F} = \{(k-1)c, \cdots, (k-1)(k-1)\}$ $(1 \leq c \leq k-1)$ of $(k-c)$ forbidden blocks.

In view of basic properties of the normalized auto-correlation 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.

We generalized this result and gave the correlational properties of the discretized Markov β-transformations with the alphabet $\Sigma = \{0, 1, \cdots, k-1\}$ and the set $\mathcal{F} = \{(k-1)(k-1)\}$ of forbidden blocks.

We also applied the generalized result to evaluate the auto-correlation function for the optimum binary spreading sequences of Markov chains based on discretized β-transformations, where $\beta = 1 + \sqrt{3}$.