2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

A Realization of Optimum Binary Spreading Sequences of Markov Chains Based on Discretized β-transformations

Hiroshi Fujisaki

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

Abstract—We construct optimum binary spreading sequences of Markov chains in terms of bit error probabilities in asynchronous spread-spectrum multiple-access (SSMA) communication systems based on discretized β-transformations. We also evaluate the normalized auto-correlation function for the optimum binary spreading sequences of Markov chains based on the discretized β-transformations. The experimental results of the bit error probabilities in the asynchronous SSMA communication systems using the obtained sequences agree with the theoretical estimations of the bit error probabilities based on the central limit theorem (CLT).

1. Introduction

Spreading sequences are a kind of pseudo-random numbers. It is one of the most crucial tasks in spread spectrum techniques to realize the optimum spreading sequences in terms of the performance of asynchronous spread-spectrum multiple-access (SSMA) communication systems where the sequences are used.

From the viewpoint of the performance of communication systems, it is bit error probabilities that are of the utmost importance as a measure of the reliability of the systems. The bit error probabilities in asynchronous SSMA communication systems were estimated by using Gaussian distributions whose variance was the average interference parameter (AIP) that was introduced by Pursley in [1] as a measure of the average signal-to-noise ratio (SNR) in asynchronous SSMA communication systems. This is the so called standard Gaussian approximation (SGA).

Chaotic spreading sequences are the sequences of pseudo-random numbers generated by one-dimensional ergodic transformations, which is one of the applications of Ulam and von Neumann's idea in [2]. It was found in [3] that a class of chaotic spreading sequences whose auto-correlations exponentially decay achieved a better performance in terms of the *mean* value of the AIP [1] as compared to Gold sequences whose auto-correlations are like a delta function. This discovery created a revolution in designing spreading sequences since sequences whose auto-correlations are like a delta function were commonly regarded as good sequences before the pioneering work. We note here that the chaotic sequences proposed in [3] are equivalent to the sequences generated by a class of Markov chains.

While Pursley defined the AIP as a measure of the average SNR in asynchronous SSMA communication systems, Yao pointed out in [4] that evaluations of bit error probabilities based on the SGA with the AIP were not valid for the systems with small numbers of users, low length of pseudonoise (PN) sequences, and high SNRs, which naturally posed the following questions: i) Why were evaluations of bit error probabilities based on the SGA with the AIP not valid for systems with small numbers of users and low lengths of PN sequences? ii) How can one give simple theoretical evaluations of bit error probabilities still valid for systems with small numbers of users and low lengths of PN sequences? These problems have often been discussed.

Motivated by the spreading sequences of Markov chains proposed in [3], we have studied to determine the optimum spreading sequences of Markov chains in terms of bit error probabilities in asynchronous SSMA communication systems. As a result of a series of studies [5]–[8], we have solved the above-mentioned Yao's questions completely in virtue of the central limit theorem (CLT) together with large deviations analysis.

We showed that the SGA with the *mean* value of the AIP for estimations of bit error probabilities in such systems was the 0-th order approximation of the evaluation based on the CLT. As far as binary spreading sequences are concerned, correlational properties of the optimum spreading sequences in terms of the mean value of the AIP obtained in [9] coincide with the properties of the optimum sequences in terms of the bit error probabilities in the systems based on the CLT. We remark here that the result in [9] only gave correlational properties of the optimum spreading sequences. It did not tell us how to design the optimum spreading sequences in terms of the mean value of the AIP.

On the other hand, based on the CLT, we determined $k\,(\geq\ 2)$-state Markov chains generating k-phase spreading sequences that minimize bit error probabilities in asynchronous SSMA communication systems in [6]. Moreover,

[1] The mean value of the AIP is averaged over spreading sequences as random variables while the original AIP defined in [1] is a random variable of spreading sequences.

we found a novel class of spreading sequences, namely the phase-shift-free $k\,(\geq 3)$-phase spreading sequences, and showed in [7] that the optimum phase-shift-free k-phase spreading sequences of Markov chains were superior to the optimum binary spreading sequences of Markov chains in terms of the bit error probabilities in the system based on the CLT.

Unfortunately, however, such existence of the optimum sequences was theoretically determined and confirmed by using the piecewise-linear Markov transformations with the help of Monte-Carlo simulations. In fact, the optimum sequences are not available for practical use like Gold sequences because the idea in [2] requires handling real numbers in its applications. More precisely, the round off errors due to the truncation of real numbers occurs while iterating the Markov transformations by using computers.

Under these unpromising circumstances, a breakthrough was made in [10], where Bernoulli transformations were suggested for SSMA communication systems. Inspired by the results in [10], we defined discretized Markov transformations and found an algorithm to give the number of full-length sequences based on the discretized Markov transformations in [11].

In [12], we defined the piecewise-monotone-increasing Markov transformations, which included not only $k\,(\geq 2)$-adic transformations but also Markov β-transformations. Besides, without knowing the total number of full-length sequences based on the discretized piecewise-monotone-increasing Markov transformations, we gave the bounded monotone truth-table algorithm for generating *all* full-length sequences which were based on the defined discretized Markov transformations.

In this report, we construct optimum binary spreading sequences of Markov chains in terms of bit error probabilities in asynchronous SSMA communication systems based on discretized β-transformations.

2. A Realization of Markov Chains with Prescribed Correlation Properties Based on β-transformations

In terms of bit error probabilities in asynchronous SSMA communication systems, the optimum $k\ (\geq\ 2)$-phase spreading sequences of Markov chains were determined in [7]. For the case where $k\ =\ 2$, the optimum binary spreading sequences of Markov chains are characterized by the sequence $(Z_n)_{n=0}^{\infty}$ of $\{1,-1\}$-valued stationary Markov chains with $\mathbb{E}[Z_n] = 0$ and $\mathbb{E}[Z_0Z_\ell] = \left(-2+\sqrt{3}\right)^{\ell}$ $(\ell \geq 0)$. For a random variable Z, we use $\mathbb{E}[Z]$ to denote the expected value of Z.

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

Definition 1 *The normalized 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 $r_N(\ell;\boldsymbol{X},\boldsymbol{Y}) = 1/N \cdot \sum_{i=0}^{N-1} X_iY_{i+\ell\,(\bmod N)}$, where $\ell = 0,1,\cdots,N-1$ and, for integers a and $b\,(\geq\ 1)$, $a\,(\bmod b)$ denotes the least residue of a to modulus b. If $\boldsymbol{X} = \boldsymbol{Y}$, we call $r_N(\ell;\boldsymbol{X},\boldsymbol{X})$ the normalized auto-correlation function, and simply denote it by $r_N(\ell;\boldsymbol{X})$.*

In order to construct the sequence $\boldsymbol{X}$ with $r_N(\ell;\boldsymbol{X}) = \left(-2+\sqrt{3}\right)^{\ell}$, we recall the notion of *Perron numbers* defined in [13] as follows.

Definition 2 *The number λ is a Perron number if i) λ is a positive algebraic integer, and ii) $\lambda > |\mu|$ for all other algebraic conjugates μ of λ. We use $\mathbb{P}$ to denote the set of Perron numbers.*

Let A be a non-negative integral matrix. If $A^n > 0$ for some positive integer n, then A is called *primitive*, which is equivalent to irreducible and aperiodic. For an primitive matrix A, we use λ_A to denote the Perron-Frobenius eigenvalue of A. Thus the Perron number is characterized by the following.

Theorem 1 (Lind [13]) *$\lambda \in \mathbb{P}$ iff $\lambda = \lambda_A$ for some primitive A.*

For our purpose, since the correlation function in question has only one parameter, it suffices to consider $\lambda \in \mathbb{P}$ with degree 2. The minimal polynomial of λ over $\mathbb{Q}$ is defined by $f(t) = t^2 - c_1t - c_2$ where $c_1, c_2 \in \mathbb{Z}$. Its companion matrix of is given by $B = \begin{pmatrix} 0 & c_2 \\ 1 & c_1 \end{pmatrix}$. Recall that the characteristic polynomial and the minimal polynomial of B are equal to $f(t)$. In order to associate a β-transformation with B, in what follows, we assume $0 < c_2 \leq c_1$.

The adjacency matrix A of the β-transformation T associated with the above companion matrix B is given by

$$A = \left(\begin{array}{ccc|ccc} \overbrace{1 & \cdots & 1}^{c_2} & 1 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1 \\ \hline 1 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right)\begin{matrix} \\ \\ \\ \left.\begin{matrix} \\ \end{matrix}\right\} c_1 \end{matrix} \overbrace{\qquad\qquad}^{c_1+1} .$$

For almost every x in $[0,1)$, the n-th iterate $T^n(x)$, where $T^0(x) = x$ and $T^n(x) = T^{n-1}(T(x))$ for $n = 1,2,\cdots$, together with a map $\Psi : [0,1) \to \{1,-1\}$ defined by $\Psi(x) = 1$ if $x < c_1/\beta$ and $\Psi(x) = -1$ otherwise, generates a sequence $(Z_n)_{n=0}^{\infty}$ of $\{1,-1\}$-valued Markov chain by setting $Z_n = \Psi(T^n(x))$. Thus we obtain $\mathbb{E}[Z_0Z_\ell] = \left\{\left(\lambda+\overline{\lambda}\right)/\left(\lambda-\overline{\lambda}\right)\right\}^2 - 4\lambda\overline{\lambda}/(\lambda-\overline{\lambda})^2 \cdot \left(\overline{\lambda}/\lambda\right)^{\ell}$ $(\ell \geq 0)$, where $\overline{\lambda}$ is the algebraic conjugate of λ, the unique integral solution (c_1,c_2) of an equation $-2+\sqrt{3} = \lambda\left/\overline{\lambda}\right. = \left\{c_1 - \sqrt{c_1^2+4c_2}\right\}\left/\left\{c_1 + \sqrt{c_1^2+4c_2}\right\}\right.$ with $0 < c_2 \leq c_1$

is given by $c_1 = c_2 = 2$. Eventually, we obtain the β-transformation T with $\beta = 1+\sqrt{3} = \lambda$ which is the positive solution of $t^2 - 2t - 2 = 0$. The graph of T is given in Fig. 1.

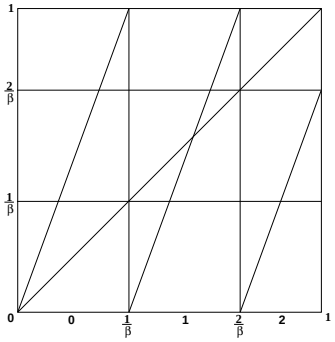

Figure 1: The β-transformation with $\beta = 1 + \sqrt{3}$.

Although we successfully obtain a sequence of $\{1,-1\}$-valued stationary Markov chain with $\mathbb{E}[Z_0 Z_\ell] = \left(-2+\sqrt{3}\right)^\ell$ ($\ell \geq 0$), we still have $\mathbb{E}[Z_n] = (\lambda+\overline{\lambda})/(\lambda-\overline{\lambda}) = 1/\sqrt{3} \neq 0$ since the stationary distribution of the chain is given by $(p_1, p_2) = 1/\left(\lambda-\overline{\lambda}\right)\cdot(-\overline{\lambda},\lambda) = 1/\left(2\sqrt{3}\right)\cdot\left(-1+\sqrt{3}, 1+\sqrt{3}\right)$, which is not uniform.

In the next section, without changing the realized correlational properties of the binary optimum spreading sequences of Markov chains, we transform the distribution (p_1, p_2) of the sequences into the uniform distribution by virtue of sliding block codes.

3. A Realization of Markov Chains with Prescribed Correlation Properties with the Uniform Distribution Based on Discretized β-transformations

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.

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 ϵ to denote the empty block. 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 shift of finite type (SFT) is a subshift that 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.

The symbolic representation of β-expansions of real numbers with $\beta = 1+\sqrt{3}$, which is realized by the iterates of the β-transformation T shown in Fig. 1, is given by the SFT $X_{\mathcal{F}} \subset \Sigma^{\mathbb{Z}}$ where $\Sigma = \{0,1,2\}$ and $\mathcal{F} = \{22\}$. Its graph representation G is given in Fig. 2 which also represents T.

Setting $G = G^{[2]}$, we obtain a sequence $(G^{[n]})_{n=2}^{\infty}$ of higher edge graphs of G. For each $n \geq 2$, we use H_n

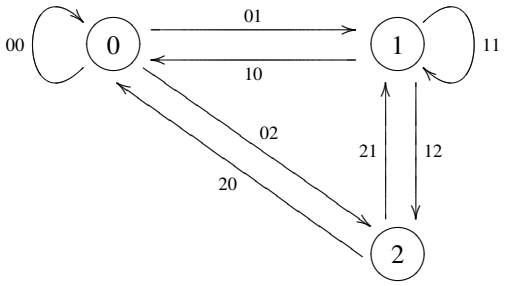

Figure 2: The graph representation G of $X_{\{22\}}$.

to denote the Eulerian subgraph spanning $G^{[n]}$ with maximal number of edges, whose Eulerian circuits are the full-length sequences based on the discretized β-transformation T with $\beta = 1+\sqrt{3}$. In Fig. 2, we see that G is Eulerian. Thus we have $G = G^{[2]} = H_2$ in this case. In the Eulerian subgraph H_2, we obtain a full-length sequence 001021120 for instance. The length $|\mathcal{B}_n|$ of full-length length sequences is given by $|\mathcal{B}_n| = \beta^n + \overline{\beta}^n$ ($n \geq 2$) in [14], where $\overline{\beta} = 1-\sqrt{3}$, which is the algebraic conjugate of β.

Now we are in the position to construct the optimum binary spreading sequences of Markov chains based on the discretized β-transformations with $\beta = 1+\sqrt{3}$.

A total order relation $\preceq$ on $\mathcal{L}(X_{\mathcal{F}}) \setminus \{\epsilon\}$ is defined by the following: for any $u = u_1\cdots u_m$ ($m \geq 1$) and $v = v_1\cdots v_n$ ($n \geq 1$) in $\mathcal{L}(X_{\mathcal{F}})$, $u \preceq v$ if and only if

$$\frac{u_1}{\beta} + \frac{u_2}{\beta^2} + \cdots + \frac{u_m}{\beta^m} \leq \frac{v_1}{\beta} + \frac{v_2}{\beta^2} + \cdots + \frac{v_n}{\beta^n}.$$

For simplicity, we use L to denote the length $|\mathcal{B}_n|$ of full-length length sequences. We define a block code $\Phi : \{0,1,2\}^L \to \{1,-1\}$ by for $v = v_1 v_2 \cdots v_L \in \{0,1,2\}^L$,

$$\Phi(v) = \begin{cases} 1 & \text{if} \quad v \preceq 02, \\ -1 & \text{if} \quad 02 \prec v \preceq 2, \\ 1 & \text{if} \quad 2 \prec v. \end{cases}$$

We use S to denote the shift transformation on $\{0,1,2\}^L$, i.e., $S(v_1, v_2, \cdots, v_{L-1}, v_L) = (v_2, v_3, \cdots, v_L, v_1)$ for $v = v_1 v_2 \cdots v_L \in \{0,1,2\}^L$. Thus we obtain a sliding block code ϕ for periodic sequences of period L defined by $\phi(v^\infty) = (\Phi(v)\Phi(Sv)\Phi(S^2 v)\cdots\Phi(S^{L-1}v))^\infty$, where $u^\infty = \cdots uuu\cdots$ for a block u. The sliding block code ϕ transform the full-length sequence over $\Sigma = \{0,1,2\}$ based on the discretized Markov β-transformation with $\beta = 1+\sqrt{3}$ into the optimum binary spreading sequences of Markov chains as follows.

Let $\boldsymbol{X}$ be a full-length sequence over $\Sigma = \{0,1,2\}$ of length $L = |\mathcal{B}_n|$ based on the discretized Markov β-transformation with $\beta = 1+\sqrt{3}$. Thus the optimum binary spreading sequence of Markov chain is realized by $\boldsymbol{Y} = \Phi(\boldsymbol{X})\Phi(S\boldsymbol{X})\Phi(S^2\boldsymbol{X})\cdots\Phi(S^{L-1}\boldsymbol{X})$.

We here give an example of the optimum binary spreading sequences of Markov chains of length $|\mathcal{B}_n|$.

Example 1 *For $n = 3$, we have $L = 20$ and*

$$00010020110121021112 \xrightarrow{\phi|_{\Sigma^L}} 11101011001010010001,$$

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

Applying the previous results in [15] to the optimum binary spreading sequences of Markov chains, we have

Theorem 2 *For* $0 \le \ell \le n-1$*, we obtain*

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

This implies $r_{|\mathcal{B}_n|}(\ell; \boldsymbol{Y}) = \mathbb{E}[Z_0 Z_\ell] + O\left(\left(\frac{\overline{\beta}}{\beta}\right)^{n}\right)$, where O is the big O notation from the Landau symbol.

4. Experimental Results

A short table of values of the length $|\mathcal{B}_n|$, the total number ν_n of the full-length sequences over $\{0,1,2\}$ in H_n, and the total number $\widetilde{\nu_n}$ of the realized optimum binary spreading sequences of Markov chains are given in Table 1, respectively.

Table 1: A short table of values of $|\mathcal{B}_n|$, ν_n, and $\widetilde{\nu_n}$.

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

Fig. 3 shows the theoretical estimations based on the CLT given in [5] and the experimental results of bit error probabilities in asynchronous SSMA communication systems using the realized optimum binary spreading sequences of Markov chains based on the discretized β-transformations as a function of the number of users J for $N = 56$. In this figure, the experimental results and the theoretical estimations based on the CLT agree properly with each other.

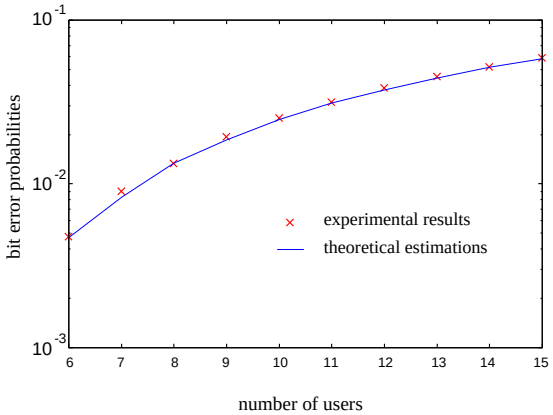

Figure 3: The bit error probabilities.

Acknowledgments

This study was supported by the Telecommunications Advancement Foundation. The author is grateful to Mr. Jinse Shimo for help with the computer simulations.

References

[1] M. B. Pursley, "Performance Evaluation for Phase-Coded Spread-Spectrum Multiple-Access Communication – Part I: System Analysis," *IEEE Trans. Commun.*, vol.COM-25, no.8, pp.795–799, 1977.

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

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

[4] K. Yao, "Error Probability of Asynchronous Spread Spectrum Multiple Access Communication Systems," *IEEE Trans. Commun.*, vol.COM-25, no.8, pp.803–809, 1977.

[5] H. Fujisaki and G. Keller, "The central limit theorem for the normalized sums of the MAI for SSMA communication systems using spreading sequences of Markov chains," *IEICE Trans. Fundamentals*, vol.E89-A, no.9, pp. 2307–2314, 2006.

[6] H. Fujisaki, "Design of Optimum M-Phase Spreading Sequences of Markov Chains," *IEICE Trans. Fundamentals*, vol.E90-A, no.10, pp. 2055–2065, 2007.

[7] H. Fujisaki and H. Sugimori, "Phase-Shift-Free M-Phase Spreading Sequences of Markov Chains," *IEEE Trans. on Circuit and Systems Part I*, vol.CAS-55, pp. 876–882, 2008.

[8] H. Fujisaki, "Performance Analysis of SSMA Communication Systems with Spreading Sequences of Markov Chains: Large Deviations Principle Versus the Central Limit Theorem," *IEEE Trans. on Information Theory*, vol. IT-57, pp. 1959–1967, 2011.

[9] R. Rovatti and G. Mazzini, "Interference in DS-CDMA systems with exponentially vanishing autocorrelations: Chaos-based spreading is optimal," *IEE Electronics Letters*, vol. 34, pp. 1911–1913, 1998.

[10] 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.

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

[12] 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.

[13] D. A. Lind, "The entropies of topological Markov shifts and a related class of algebraic integers," *Ergodic Theory and Dynamical Systems*, vol. 4, pp. 283-—300, 1984.

[14] H . Fujisaki, "On the topological entropy of the discretized Markov β-transformations," submitted to *IEICE Trans. Fundamentals*, total 10 pages, 2016.

[15] H. Fujisaki, "Correlational Properties of the Full-Length Sequences Based on the Discretized Markov β-transformations," submitted to *NOLTA, IEICE*, total 11 pages, 2016.