2010 International Symposium on Nonlinear Theory and its Applications
NOLTA2010, Krakow, Poland, September 5-8, 2010

Spreading Sequences with Negative Auto-correlation Based on Chaos Theory and Gold Sequences — Increase of Family Sizes and Performance Evaluation —

Akio Tsuneda and Taizo Sagara

Department of Computer Science and Electrical Engineering, Kumamoto University
2–39–1 Kurokami, Kumamoto, 860–8555 JAPAN
E-mail: tsuneda@cs.kumamoto-u.ac.jp

Abstract—Spreading sequences with appropriate negative auto-correlation can reduce average multiple access interference (MAI) in asynchronous DS/CDMA systems compared with the conventional spreading sequences such as Gold sequences generated by linear feedback shift registers (LFSRs). We design spreading sequences with negative auto-correlation based on Gold sequences and the chaos theory for the Bernoulli map. The family size of the proposed sequences is 6 times as large as that of the original Gold sequences. By computer simulations, we evaluate BER performances of asynchronous DS/CDMA systems using the proposed sequences.

1. Introduction

Linear feedback shift register (LFSR) sequences (*e.g.*, M-sequences, Gold sequences, Kasami sequences) are the most well-known pseudo-random sequences and they are practically used for spreading sequences in direct-sequence code division multiple access (DS/CDMA) systems [1].

Many types of spreading sequences have been proposed for enhancement of system performance such as bit error rate (BER). Especially, it is remarkable that spreading sequences with exponentially vanishing negative auto-correlations can reduce multiple access interference (MAI) in asynchronous DS/CDMA systems compared with classical spreading codes such as M-sequences, Gold sequences and Kasami sequences [2],[3]. Such negatively auto-correlated sequences can be generated by using one-dimensional nonlinear chaotic maps, which are called *chaotic sequences* [2]–[4]. Their discretized version called *maximal-period sequences* has also been considered [5].

Furthermore, we designed binary sequences with negative (but not exponentially vanishing) auto-correlation based on the well-known Bernoulli and tent maps [6]. Theoretically, the performances of such sequences are slightly worse than the sequences with exponentially vanishing negative auto-correlations with respect to MAI reduction. However, the proposed sequences can be generated by simpler chaotic maps than the others, though our binary functions are somewhat complex. Noting that the Bernoulli/tent maps with finite bits can be realized by a class of nonlinear feedback shift registers (NFSRs) [7], we proposed NFSR-based generators of negatively auto-correlated binary sequences and revealed that the proposed sequences can also reduce BER in asynchronous DS/CDMA systems compared with conventional Gold sequences [6]. However, the circuit scale of NFSRs is, in general, much larger than LFSRs.

We also designed periodic binary sequences with negative auto-correlation based on Gold sequences generated by two LFSRs [8]. Namely, we designed such sequences based on the chaos theory for the Bernoulli map because random binary sequences can also be regarded as finite-bit approximation of the Bernoulli map [8]. By computer simulations, we revealed that the proposed sequences can reduce BER in asynchronous DS/CDMA communications [9].

In this paper, we also design periodic binary sequences with negative auto-correlation based on the chaos theory and Gold sequences, where the family size of the proposed sequences is 6 times as large as that of the original Gold sequences [10]. By computer simulations, we investigate BER performances of the proposed sequences in asynchronous DS/CDMA communications.

2. Chaos-Based Sequences and Their Performance

In asynchronous DS/CDMA systems, the average interference parameter (AIP) is defined by [11]

$$r_{k,i} = 2N^2 + 4\sum_{l=1}^{N-1} A_k(\ell)A_i(\ell) + \sum_{l=1-N}^{N-1} A_k(\ell)A_i(\ell+1), \quad (1)$$

where $A_k(\ell)$ is an aperiodic auto-correlation function of the k-th user's spreading sequence $\{B_n^{(k)}\}_{n=0}^{N-1}$ with period N, defined by

$$A_k(\ell) = \begin{cases} \displaystyle\sum_{n=0}^{N-1-\ell} B_n^{(k)} B_{n+\ell}^{(k)} & (0 \le \ell \le N-1) \\ \displaystyle\sum_{n=0}^{N-1+\ell} B_{n-\ell}^{(k)} B_n^{(k)} & (1-N \le \ell < 0) \\ 0 & (|\ell| > N). \end{cases} \quad (2)$$

Now we briefly introduce generation of chaotic sequences and their statistical analyses. Using one-dimensional nonlinear difference equation defined by

$$x_{n+1} = \tau(x_n),\ x_n \in I = [d, e],\ n = 0, 1, 2, \cdots, \quad (3)$$

we can generate a *chaotic* real-valued sequence $\{x_n\}_{n=0}^{\infty}$, where $x_n = \tau^n(x_0)$. We transform such a real-valued sequence into a binary sequence $\{\beta(\tau^n(x))\}_{n=0}^{\infty}$ ($\beta(x) \in \{-1, 1\}$). The theoretical auto-correlation function of such a binary sequence $\{\beta(\tau^n(x))\}_{n=0}^{\infty}$ is defined by

$$C(\ell;\beta) = E[\beta(x)\beta(\tau^{\ell}(x))] = \int_I \beta(x)\beta(\tau^{\ell}(x))f^*(x)dx \quad (4)$$

under the assumption that $\tau(x)$ has an invariant density function $f^*(x)$, where $E[\cdot]$ denotes the expectation. Assume that K users use chaotic binary sequences $\{\beta(\tau^n(x^{(i)}))\}_{n=0}^{N-1}$ ($i = 1, 2, \cdots, K$) of length N as their spreading codes, where the initial values $x^{(1)}, x^{(2)}, \cdots, x^{(K)}$ are statistically independent of each other. The average interference parameter (AIP) for a user in such a system is given by

$$\hat{r} = 2N^2 + 4\sum_{l=1}^{N-1}(N-\ell)^2 C(\ell;\beta)^2 + 2\sum_{l=1}^{N-1}(N-\ell)(N-\ell+1)C(\ell;\beta)C(\ell-1;\beta). \quad (5)$$

Note that eq.(5) is obtained by averaging eq.(1) with the invariant density $f^*(x)$. We also define a normalized AIP by

$$R = \lim_{N\to\infty} \frac{\hat{r}}{2N^2}. \quad (6)$$

Obviously, we have $R = 1$ for uncorrelated sequences with $C(\ell;\beta) = 0$ ($\ell \geq 1$).

First, consider the case $C(\ell;\beta) = \lambda^{\ell}$ ($|\lambda| < 1$), that is, chaotic sequences with exponentially vanishing auto-correlations. In this case, we have

$$R = \frac{\lambda^2 + \lambda + 1}{1 - \lambda^2} \quad (7)$$

which takes the minimum value $\frac{\sqrt{3}}{2}(\simeq 0.866)$ when $\lambda = -2 + \sqrt{3}$ [2],[3]. Thus such sequences have smaller AIPs than uncorrelated sequences with $R = 1$.

Next consider the sequences whose auto-correlation function is given by

$$C(\ell;\beta) = \begin{cases} 1 & (\ell = 0) \\ \varepsilon & (\ell = 1) \\ 0 & (\ell \geq 2), \end{cases} \quad (8)$$

where $|\varepsilon| < 1$. In this case, we have

$$R = 2\varepsilon^2 + \varepsilon + 1. \quad (9)$$

The minimum value of R is $\frac{7}{8}(= 0.875)$ when $\varepsilon = -\frac{1}{4}$, which is slightly larger than $\frac{\sqrt{3}}{2}(\simeq 0.866)$ of the optimum case $C(\ell;\beta) = \lambda^{\ell}$ with $\lambda = -2 + \sqrt{3}$ but the difference is quite small. Of course, the sequences of this case ($\varepsilon = -\frac{1}{4}$) also outperform the uncorrelated sequences.

Several types of chaotic maps which can generate chaotic sequences with exponentially vanishing auto-correlations are known [3],[4]. Most of them are piecewise linear Markov maps. Here, we consider the Bernoulli map $\tau_B(x)$ defined by

$$\tau_B(x) = \begin{cases} 2x & (0 \leq x < \frac{1}{2}) \\ 2x - 1 & (\frac{1}{2} \leq x \leq 1), \end{cases} \quad (10)$$

which is one of the simplest piecewise linear chaotic maps with the interval $I = [0, 1]$ and $f^*(x) = 1$. Furthermore, we define six binary functions by [10]

$$\begin{cases} B_1'(x) = \Theta_{\frac{1}{4}}(x) - \Theta_{\frac{5}{8}}(x) + \Theta_{\frac{3}{4}}(x) - \Theta_{\frac{7}{8}}(x) \\ B_2'(x) = \Theta_{\frac{1}{8}}(x) - \Theta_{\frac{1}{2}}(x) + \Theta_{\frac{3}{4}}(x) - \Theta_{\frac{7}{8}}(x) \\ B_3'(x) = \Theta_{\frac{1}{4}}(x) - \Theta_{\frac{5}{8}}(x) + \Theta_{\frac{7}{8}}(x) \\ B_4'(x) = \Theta_{\frac{1}{8}}(x) - \Theta_{\frac{3}{8}}(x) + \Theta_{\frac{3}{4}}(x) \\ B_5'(x) = \Theta_{\frac{1}{8}}(x) - \Theta_{\frac{1}{4}}(x) + \Theta_{\frac{3}{8}}(x) - \Theta_{\frac{3}{4}}(x) \\ B_6'(x) = \Theta_{\frac{1}{8}}(x) - \Theta_{\frac{1}{4}}(x) + \Theta_{\frac{1}{2}}(x) - \Theta_{\frac{7}{8}}(x), \end{cases} \quad (11)$$

where $\Theta_t(x)$ is a threshold function defined by

$$\Theta_t(x) = \begin{cases} 0 & (x < t) \\ 1 & (x \geq t). \end{cases} \quad (12)$$

Here, we define $B_i(x) = 2B_i'(x) - 1$ ($i = 1, 2, \cdots, 6$) for transformation $\{0, 1\} \to \{-1, 1\}$. By the chaos theory for the Bernoulli map, we can show that the auto-correlation function of the chaotic binary sequences $\{B_i(\tau_B^n(x))\}_{n=0}^{\infty}$ ($i = 1, 2, \cdots, 6$) is given by

$$C(\ell; B_i) = \begin{cases} 1 & (\ell = 0) \\ -\frac{1}{4} & (\ell = 1) \\ 0 & (\ell \geq 2). \end{cases} \quad (13)$$

This implies that the sequences $\{B_i(\tau_B^n(x))\}_{n=0}^{\infty}$ are *optimal* spreading codes in a class of sequences with the auto-correlation function given by eq.(8).

3. Negatively Correlated Sequences Based on Gold Sequences

3.1. Gold Sequences and Proposed Generator

Gold sequences can be generated by two k-stage linear feedback shift registers (LFSRs) generating preferred pairs of M-sequences [1]. Let $\{g_n\}_{n=0}^{N-1}$ be an Gold sequence, where $g_n \in \{0, 1\}$ and $N = 2^k - 1$. The family size of the Gold sequences is $2^k + 1$ including the original preferred pairs of M-sequences [1]. If we observe m successive bits of a Gold sequence, we get a decimal integer by

$$x_n = g_n \cdot 2^{m-1} + g_{n-1} \cdot 2^{m-2} + \cdots + g_{n-m+1} \cdot 2^0. \quad (14)$$

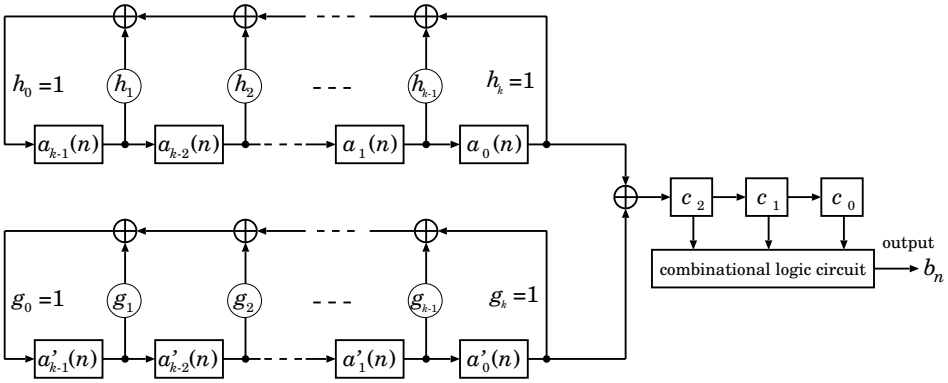


Figure 1: Proposed sequence generator based on Gold sequences

By plotting (x_n, x_{n+1}), we obtain a one-dimensional (1-D) map (so called, *return map*) of the Gold sequence. We can easily confirm that the shape of such a 1-D map (return map) is similar to the Bernoulli map [8],[9]. In this sense, the chaos theory can be applied to the Gold sequences.

Thus, we propose a sequence generator based on LFSRs generating Gold sequences as shown in Fig.1, where the output binary sequence $\{b_n^{(i)}\}$ is obtained by

$$b_n^{(i)} = \begin{cases} 1 & c_0c_1c_2 \in B_i \\ 0 & \text{otherwise,} \end{cases} \tag{15}$$

where

$$\begin{cases} B_1 = \{010, 011, 100, 110\} \\ B_2 = \{001, 010, 011, 110\} \\ B_3 = \{010, 011, 100, 111\} \\ B_4 = \{001, 010, 110, 111\} \\ B_5 = \{001, 011, 100, 101\} \\ B_6 = \{001, 100, 101, 110\}. \end{cases} \tag{16}$$

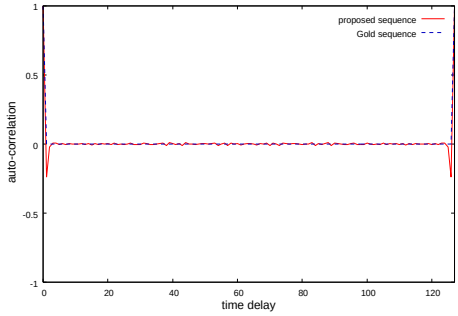
which correspond to the binary functions given by eq.(11), that is, the binary sequence $\{2b_n^{(i)} - 1\}$ is finite-bit approximation of the chaotic binary sequence $\{B_i(\tau_B^n(x))\}_{n=0}^{\infty}$ with the correlation function of eq.(13). Hence, the proposed generator is expected to generate negatively correlated binary sequences similar to the chaotic binary sequences.

Also it should be noted that the family size of the proposed sequences is 6 times as large as that of the original Gold sequences, *i.e.,* $(2^k + 1) \times 6$, by using the 6 binary (logic) functions for every Gold sequence.

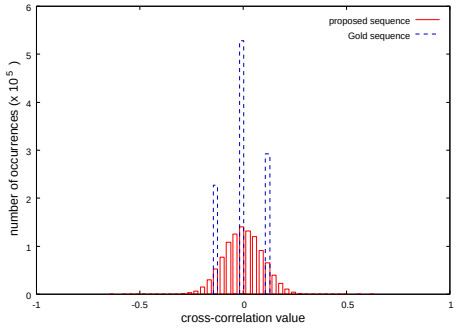
3.2. Correlation Properties

Next, we investigated correlation properties of the proposed sequences. Fig.2 (a) shows the average auto-correlation function of the proposed sequences for $k = 7$, where the auto-correlation values are averaged for 129 sequences randomly chosen from a family of the sequences. It is shown that the average auto-correlation function is almost equal to the theoretical one.

Fig.2 (b) shows the distribution of the cross-correlation values of the proposed sequences for $k = 7$, where all the possible pairs of the 129 sequences are taken into account. The cross-correlations of 129 original Gold sequences are also shown in the figure. The distribution is similar to the Gaussian distribution with 0 mean and the maximum cross-correlation value is larger than that of Gold sequences.



(a) Average auto-correlation function



(b) Distribution of cross-correlation values

Figure 2: Auto-/Cross-correlation properties of the proposed sequences based on Gold sequences ($k = 7$)

3.3. Simulations of Asynchronous DS/CDMA

We performed computer simulations of asynchronous DS/CDMA communications using the proposed sequences. In these simulations, the number of transmitted information bits per user is $1,000$ and there are random delays be-

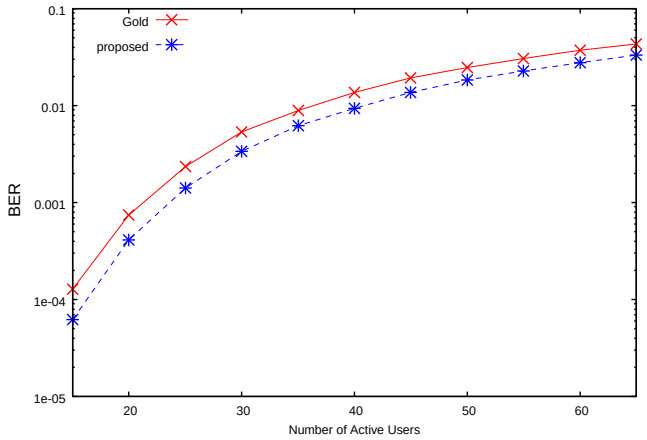


Figure 3: BER performances of the proposed sequences in asynchronous DS/CDMA communications ($k = 7$)

tween each user. We also assume that there is no channel noise in order to focus on BER performances depending on spreading sequences. The simulations were performed $1,000$ times by changing initial values of random numbers and the averages of BERs were computed. The length of spreading sequences is set to $N = 127$ ($k = 7$).

The results are shown in Fig.3, where the performance of Gold sequences is also shown for comparison. We can find that the BER performance of the proposed sequences obviously outperforms Gold sequences.

4. Concluding Remarks

We have designed spreading sequences with negative auto-correlation based on the well-known LFSR sequences (Gold sequences). The design is based on the chaos theory for the Bernoulli map. By computer simulations of asynchronous DS/CDMA communications, we have shown that the proposed sequences can reduce the BER compared with the original Gold sequences. The proposed sequence generator is obtained just by adding a combinational logic circuit with 3 inputs and 1 output to the Gold sequence generator. Furthermore, the family size of the proposed sequences is 6 times as large as that of the original Gold sequences. Hence, we can conclude that the proposed sequences are very useful for asynchronous DS/CDMA communication systems.

Acknowledgments

This work was partly supported by The Telecommunications Advancement Foundation of Japan.

References

[1] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Research Studies Press, 1996.

[2] R. Rovatti and G. Mazzini, "Interference in DS-CDMA Systems with Exponentially Vanishing Autocorrelations: Chaos-Based Spreading Is Optimal," *Electronics Letters*, Vol.34, No.20, pp.1911–1913, 1998.

[3] G. Mazzini, R. Rovatti, G. Setti, "Interference Minimization by Auto-correlation Shaping in Asynchronous DS-CDMA Systems: Chaos-based Spreading is Nearly Optimal," *Electronics Letters*, Vol.35, No.13, pp.1054–1055, 1999.

[4] A. Tsuneda, "Design of Binary Sequences With Tunable Exponential Autocorrelations and Run Statistics Based on One-Dimensional Chaotic Maps," *IEEE Trans. Circuits Syst. I*, vol.52, no.2, pp.454–462, 2005.

[5] 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, 2003.

[6] A. Tsuneda, D. Yoshioka, and T. Hadate, "Design of Spreading Sequences with Negative Auto-Correlations Realizable by Nonlinear Feedback Shift Registers," *Proc. of IEEE ISSSTA 2004*, pp.330-334, 2004.

[7] 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, 2002.

[8] A. Tsuneda and Y. Miyazaki, "Design and Evaluation of Spreading Sequences with Negative Auto-correlations Based on Chaos Theory and LFSR Sequences," *Proc. IEEE ISSSTA 2008*, CD-ROM, 2008.

[9] A. Tsuneda and Y. Miyazaki, "Performance Evaluation of Spreading Sequences with Negative Auto-correlation Based on Chaos Theory and Gold Sequences," *Proc. The Fourth International Workshop on Signal Design and Its Applications in Communications*, CD-ROM, pp.169–172, 2009.

[10] A. Tsuneda, K. Kubo, and Y. Miyazaki, "Design and Evaluation of Spreading Sequences with Negative Auto-correlation Based on Chaos Theory and M-Sequences," *Proc. ITC-CSCC 2009*, CD-ROM, pp.1040–1043, 2009.

[11] 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.