PAPER Special Section on Signal Design and its Application in Communications

Binary Spreading Sequences with Negative Auto-Correlation Based on Chaos Theory and Gold Sequences for Application to Asynchronous DS/CDMA Communications

Akio TSUNEDA[†a)], ***Member and*** **Yasunori MIYAZAKI**[†*], ***Nonmember***

SUMMARY Spreading sequences with appropriate negative auto-correlation can reduce average multiple access interference (MAI) in asynchronous DS/CDMA systems compared with the conventional 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. By computer simulations, we evaluate BER performances of asynchronous DS/CDMA systems using the proposed sequences.

key words: *asynchronous DS/CDMA, negative auto-correlation, gold sequence, chaos theory*

1. Introduction

Many types of spreading sequences have been proposed for direct-sequence code division multiple access (DS/CDMA) systems, and the most well-known sequences are linear feedback shift register (LFSR) sequences (e.g., M-sequences, Gold sequences, Kasami sequences) [1]. 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 Gold sequences [2], [3]. Such negatively auto-correlated sequences can be generated by using one-dimensional nonlinear chaotic maps, which are called *chaotic sequences* [3]–[6]. Their discretized version called *maximal-period sequences* has also been considered [7].

Furthermore, we designed binary sequences with a negative (but not exponentially vanishing) auto-correlation based on the well-known Bernoulli and tent maps [8]. 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) [9], [10], 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 the conventional Gold sequences [8]. However, the circuit scale of NFSRs is, in general, much larger than LFSRs.

In this paper, we design periodic binary sequences with negative auto-correlation based on Gold sequences generated by two LFSRs in a similar manner to the NFSR-based sequences in [8]. Namely, we design 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. By numerical experiments, we investigate auto-/cross-correlation properties of the proposed sequences [11]. Furthermore, we also investigate BER performances of the proposed sequences in asynchronous DS/CDMA communications by computer simulations [12].

2. Chaos-Based Sequences with Negative Auto-Correlations and Their Performance

In asynchronous DS/CDMA systems, the average interference parameter is defined by [13], [14]

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

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

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

Using Eq. (1), the average signal-to-noise ratio (SNR) at the output of a correlation receiver of the i-th user among K users under additive white Gaussian noise (AWGN) environment is defined by

$$\mathrm{SNR}_i = \left\{ \frac{1}{6N^3} \sum_{k=1, k\neq i}^{K} r_{k,i} + \frac{N_0}{2E_b} \right\}^{-1}, \qquad (3)$$

Manuscript received January 14, 2010.

Manuscript revised May 20, 2010.

[†]The authors are with the Department of Computer Science and Electrical Engineering, Kumamoto University, Kumamoto-shi, 860-8555 Japan.

[*]Presently with Toyota Motor Kyushu, Inc.

a) E-mail: tsuneda@cs.kumamoto-u.ac.jp

DOI: 10.1587/transfun.E93.A.2307

where $N_0/2$ is two-sided spectrum density and E_b is data bit energy. The average BER for the i-th user is approximated by $P_e^i = Q(\sqrt{\mathrm{SNR}_i})$ under the assumption that the distribution of MAI is Gaussian, where $Q(x) = \int_x^\infty e^{-u^2/2}du$ [13].

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

$$x_{n+1} = \tau(x_n),\ x_n \in I = [d, e],\ n = 0, 1, 2, \cdots, \quad (4)$$

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

$$C(\ell;\beta) = E[\beta(x)\beta(\tau^\ell(x))] = \int_I \beta(x)\beta(\tau^\ell(x))f^*(x)dx \quad (5)$$

under the assumption that $\tau(\cdot)$ 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 $x^{(1)}, x^{(2)}, \cdots, x^{(K)}$ are statistically independent of each other. The average interference parameter (AIP) for a user in such a system is given by

$$\begin{aligned}\hat{r} &= 2N^2 + 4\sum_{l=1}^{N-1}(N-\ell)^2 C(\ell;\beta)^2 \\ &\quad + 2\sum_{l=1}^{N-1}(N-\ell)(N-\ell+1)C(\ell;\beta)C(\ell-1;\beta). \quad (6)\end{aligned}$$

Note that Eq. (6) is obtained by averaging Eq. (1) with the invariant density $f^*(x)$. We also define a normalized AIP by

$$R = \lim_{N\to\infty} \frac{\hat{r}}{2N^2}. \quad (7)$$

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

$$R = \frac{\lambda^2 + \lambda + 1}{1 - \lambda^2} \quad (8)$$

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

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

$$C(\ell;\beta) = \begin{cases} 1 & (\ell = 0) \\ \varepsilon & (\ell = 1) \\ 0 & (\ell \geq 2), \end{cases} \quad (9)$$

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

$$R = 2\varepsilon^2 + \varepsilon + 1. \quad (10)$$

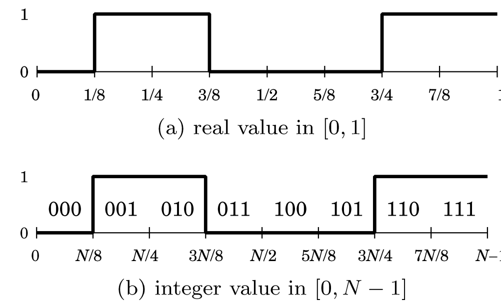


Fig. 1 Binary functions for negative correlation.

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) in the case of $C(\ell;\beta) = \lambda^\ell$ 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 with $R = 1$.

Several types of chaotic maps which can generate chaotic sequences with exponentially vanishing auto-correlations are known [3]–[6]. Most of them are piecewise linear Markov maps. Here, we consider the Bernoulli map $\tau_B(x)$ defined by

$$\tau_B(x) = \begin{cases} 2x & (0 \leq x < \frac{1}{2}) \\ 2x - 1 & (\frac{1}{2} \leq x \leq 1), \end{cases} \quad (11)$$

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

$$B'(x) = \Theta_{\frac{1}{8}}(x) - \Theta_{\frac{3}{8}}(x) + \Theta_{\frac{3}{4}}(x), \quad (12)$$

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

$$\Theta_t(x) = \begin{cases} 0 & (x < t) \\ 1 & (x \geq t). \end{cases} \quad (13)$$

The function $B'(x)$ is illustrated in Fig. 1(a). Here we define $B(x) = 2B'(x) - 1$ for transformation $\{0, 1\} \to \{-1, 1\}$. We have shown that the chaotic binary sequence $\{B(\tau_B^n(x))\}_{n=0}^\infty$ generated by the Bernoulli map has the auto-correlation function given by [8]

$$C(\ell; B) = \begin{cases} 1 & (\ell = 0) \\ -\frac{1}{4} & (\ell = 1) \\ 0 & (\ell \geq 2). \end{cases} \quad (14)$$

This implies that the sequences $\{B(\tau_B^n(x))\}_{n=0}^\infty$ are *optimal* spreading codes in a class of sequences with the auto-correlation function given by Eq. (9).

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 $N = 2^k - 1$. If we observe m successive bits of a Gold sequence, we get a decimal integer by

$$x_n = g_n \cdot 2^{m-1} + g_{n+1} \cdot 2^{m-2} + \cdots + g_{n+m-1} \cdot 2^0. \quad (15)$$

By plotting (x_n, x_{n+1}), we obtain a one-dimensional (1-D) map (so called, *return map*) of the Gold sequence. Figure 2(a) shows an example of such 1-D maps of Gold sequences, where $k = 7$ and $m = 7$. The distribution of such x_n in one period ($N = 127$) is shown in Fig. 2(b). Note that x_n does not take all possible values ($\{0, 1, \cdots, 127\}$ in this case) and its distribution is non-uniform because the period of the m-bit sequence obtained from Gold sequences are not maximal. However, the shape of the 1-D map is similar to the Bernoulli map defined by Eq. (11), which is easy to understand by noting that $x_{n+1} = g_{n+1} \cdot 2^{m-1} + g_{n+2} \cdot 2^{m-2} + \cdots + g_{n+m} \cdot 2^0$ can be expressed by

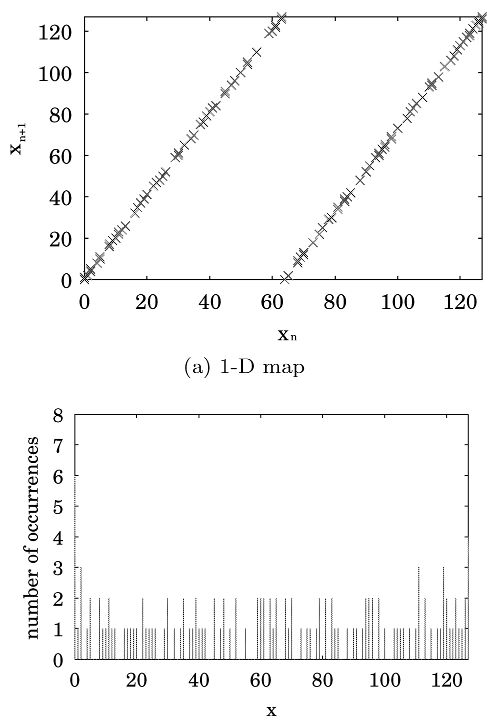
$$x_{n+1} = \begin{cases} 2x_n + g_{n+m} & (g_n = 0) \\ 2x_n + g_{n+m} - 2^m & (g_n = 1). \end{cases} \quad (16)$$

This can also be applied to general random (or pseudo-random) binary sequences. In this sense, the chaos theory for the Bernoulli map can be applied to the Gold sequences.

Thus, we propose a sequence generator based on LFSRs generating Gold sequences as shown in Fig. 3, where the output binary sequence $\{b_n\}$ is obtained by

$$b_n = \begin{cases} 1 & c_0c_1c_2 \in \{001, 010, 110, 111\} \\ 0 & \text{otherwise}, \end{cases} \quad (17)$$

which is based on the relation between Figs. 1(a) and (b). In Fig. 1(b), the most 3 significant bits are indicated for integers in each subintervals. Namely, Eq. (17) corresponds to the binary function given by Eq. (12) and the binary sequence $\{2b_n - 1\}$ is finite-bit approximation of the chaotic binary sequence $\{B(\tau_B^n(x))\}_{n=0}^{\infty}$ with the auto-correlation function of Eq. (14). Hence, the proposed generator is expected to generate negatively auto-correlated binary sequences similar to the chaotic binary sequences.



(a) 1-D map

(b) Distribution of x_n in a period

Fig. 2 Properties of Gold sequences ($k = 7$, $m = 7$).

3.2 Correlation Properties

Next, we investigate correlation properties of the proposed sequences. Figure 4(a) shows the average auto-correlation function of the proposed sequences for $k = 6$, where the auto-correlation values are averaged for 65 sequences in a *family* of the sequences. Note that a family of Gold sequences consists of $2^k + 1$ sequences including the original two M-sequences [1]. It is shown that the average auto-correlation function is almost equal to the theoretical one given by Eq. (14).

Figure 4(b) shows the distribution of the cross-correlation values of the proposed sequences for $k = 6$, where all the possible pairs of the 65 sequences are taken into account. The cross-correlations of 65 original Gold

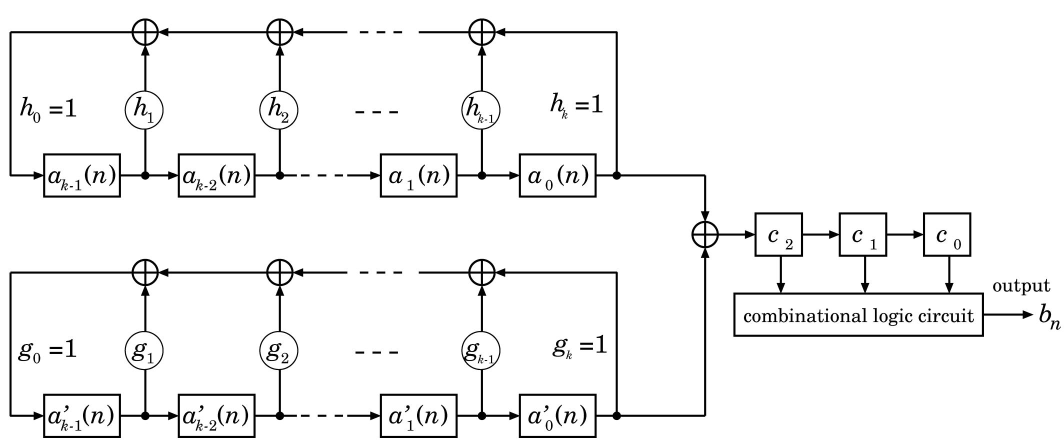
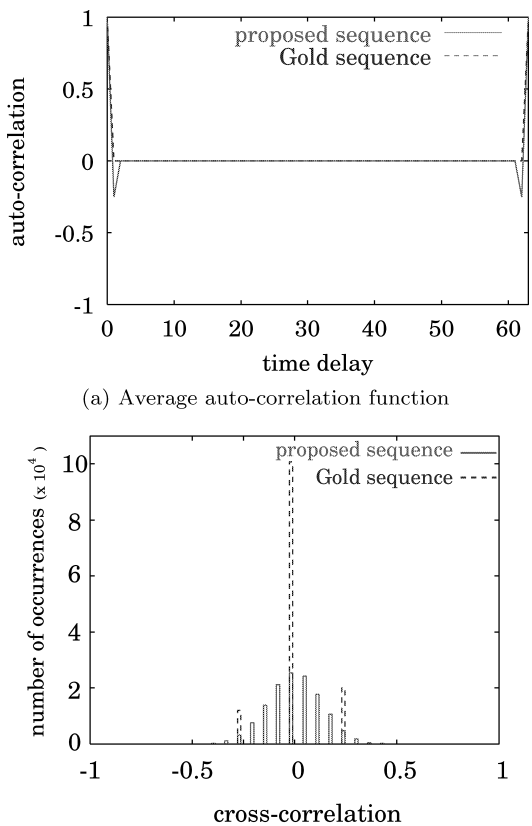


Fig. 3 Proposed sequence generator based on Gold sequences.



(a) Average auto-correlation function

(b) Distribution of cross-correlation values

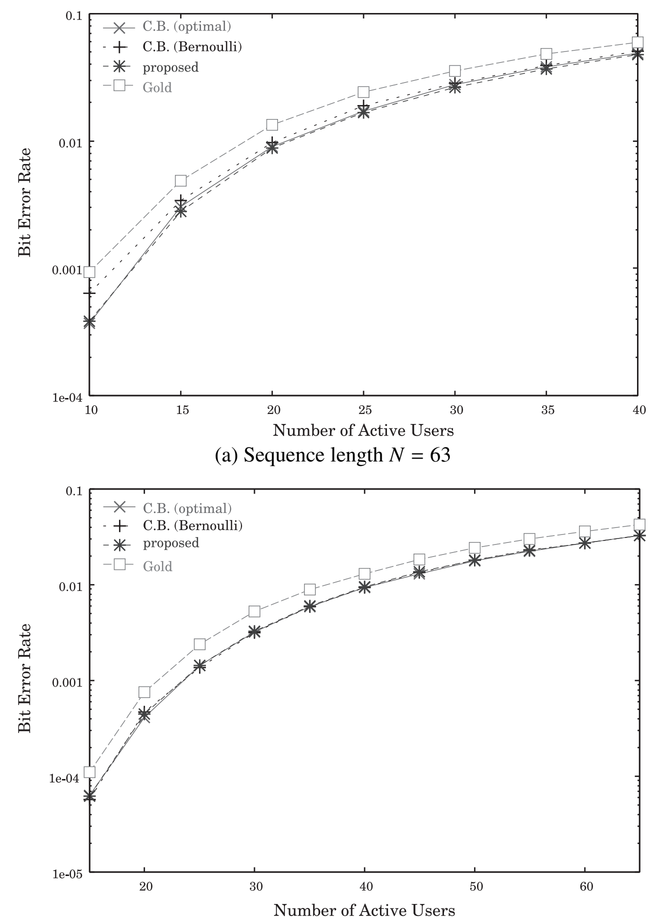
Fig. 4 Auto-/Cross-correlation properties of the proposed sequences based on Gold sequences ($k = 6$).

sequences are also shown in the figure. The distribution is similar to the Gaussian distribution with 0 mean. The maximum cross-correlation value is larger than that of Gold sequences. However, the rates of occurrences of cross-correlations larger than the maximum cross-correlation of Gold sequences are quite small.

3.3 Simulations of Asynchronous DS/CDMA

We performed computer simulations of asynchronous DS/CDMA communications using the proposed sequences as spreading codes. In these simulations, the number of transmitted information bits per user is $1,000$ and there are random delays between 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 $N = 63$ and 127.

For comparison, we also used Gold sequences and two types of chaotic binary sequences computed by sufficient precision (64-bit floating point operation). One type of chaotic sequences has the exponentially vanishing *optimal* auto-correlations ($\lambda = -2 + \sqrt{3}$) and another type has the auto-correlations given by Eq. (14) realized with the Bernoulli map. Here we used a 3-segment piecewise linear map for generating sequences with the exponentially vanishing auto-correlation function [6].



(a) Sequence length $N = 63$

(b) Sequence length $N = 127$

Fig. 5 BER performances of the proposed sequences and other sequences in asynchronous DS/CDMA communications.

The results are shown in Fig. 5, where the chaotic binary sequences are denoted by "C.B.". We can find that the BER performances of the proposed sequences are almost equal to those of chaotic binary sequences with the auto-correlation functions of Eq. (14) (*Bernoulli*) which are also almost equal to those of the *optimal* chaotic binary sequences. Furthermore, the proposed sequences obviously outperform 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. Numerical experiments showed that the auto-correlation functions of the proposed binary sequences are similar to the theoretical one given by the chaos theory. On the other hand, the distributions of cross-correlation values are similar to the Gaussian distribution with 0 mean. The maximum cross-correlation value is larger than that of Gold sequences. However, the rates of occurrences of cross-correlations larger than the maximum cross-correlation of Gold sequences are quite small.

Furthermore, 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. Hence, we can conclude that the proposed sequences are very useful for asynchronous DS/CDMA communication systems.

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,” Electron. Lett., vol.34, no.20, pp.1911–1913, 1998.
[3] G. Mazzini, R. Rovatti, and G. Setti, “Interference minimization by auto-correlation shaping in asynchronous DS-CDMA systems: Chaos-based spreading is nearly optimal,” Electron. Lett., vol.35, no.13, pp.1054–1055, 1999.
[4] T. Kohda and H. Fujisaki, “Kalman’s recognition of chaotic dynamics in designing Markov information sources,” IEICE Trans. Fundamentals, vol.E82-A, no.9, pp.1747–1753, Sept. 1999.
[5] L. Cong and L. Shaoqian, “Chaotic spreading sequences with multiple access performance better than random sequences,” IEEE Trans. Circuits Syst. I, vol.47, no.3, pp.394–397, 2000.
[6] 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.
[7] 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.
[8] A. Tsuneda, D. Yoshioka, and T. Hadate, “Design of spreading sequences with negative auto-correlations realizable by nonlinear feedback shift registers,” Proc. IEEE ISSSTA 2004, pp.330–334, 2004.
[9] S.W. Golomb, Shift Register Sequences, revised ed., Aegean Park Press, 1982.
[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, no.6, pp.1327–1332, June 2002.
[11] 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.
[12] A. Tsuneda and Y. Miyazaki, “Performance evaluation of spreading sequences with negative auto-correlation based on chaos theory and gold sequences,” Proc. Fourth International Workshop on Signal Design and Its Applications in Communications, pp.169–172 (CD-ROM), 2009.
[13] 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.
[14] M.B. Pursley and D.V. Sarwate, “Performance evaluation for phase-coded spread spectrum multiple-access communication — Part II: Code sequence analysis,” IEEE Trans. Commun., vol.COM-25, no.8, pp.800–802, 1977.

Akio Tsuneda was born in Nagasaki, Japan, in 1967. He received the B.E., M.E. and D.E. degrees in Computer Science and Communication Engineering from Kyushu University, Fukuoka, Japan, in 1990, 1992, and 1995, respectively. From 1995 to 1996, he was with the Department of Computer Science and Communication Engineering, Kyushu University. He is currently an Associate Professor of Computer Science and Electrical Engineering at Kumamoto University, Japan. During 2003–2004, he spent 8 months at University of California at Berkeley and 2 months at University of Birmingham in UK as a visiting scholar. His research interests include nonlinear dynamical systems, chaos circuits, pseudo-random sequences, and digital communications. Dr. Tsuneda is a member of IEEE, IEEJ, and SITA.

Yasunori Miyazaki was born in Kumamoto, Japan, in 1984. He received the B.E. and M.E. degrees in Computer Science and Electrical Engineering from Kumamoto University, Kumamoto, Japan, in 2007 and 2009, respectively. He was engaged in research on spreading sequences based on linear feedback shift registers and chaos theory for applications to CDMA communications. In 2009, he joined Toyota Motor Kyushu, Inc.