Search Algorithm of Maximal-Period Sequences Based on One-Dimensional Maps with Finite Bits and Its Application to DS-CDMA Systems

Daisaburou Yoshioka, Akio Tsuneda, and Takahiro Inoue

Department of Electrical and Computer Engineering, Kumamoto University
2–39–1 Kurokami, Kumamoto 860-8555, Japan
Tel: +81-96-342-3853, Fax: +81-96-342-3630
E-mail: yoshioka@st.eecs.kumamoto-u.ac.jp, tsuneda@eecs.kumamoto-u.ac.jp

Abstract: This paper presents design of spreading codes for asynchronous DS-CDMA systems. We have been trying to generate maximal-period sequences based on one-dimensional maps with finite bits whose shapes are similar to piecewise linear chaotic maps. We propose an efficient search algorithm finding such maximal-period sequences. This algorithm makes it possible to find many kinds of maximal-period sequences with sufficiently long period for CDMA applications. We also investigate bit error rate(BER) in asynchronous DS-CDMA systems using the maximal-period binary sequences by computer simulations.

1. Introduction

Code division multiple access(CDMA) systems based on spread spectrum(SS) techniques have been developed as a key technology for the third generation(3G) of cellular communication systems. In direct-sequence CDMA (DS-CDMA) systems, spreading sequences play an important role since they dominate the system performance such as bit error rate(BER). In general, spreading sequences are desired to have auto-correlation properties like a delta function for synchronization and low cross-correlations to reduce co-channel interferences causing bit errors. Furthermore, many kinds of sequences are required for increasing subscribers. As conventional spreading sequences, shift register sequences such as M-sequences, Gold sequences, and Kasami sequences are known [1].

Recently, there have been many attempts to use chaotic sequences as spreading sequences. As is well known, chaos is random behavior generated by deterministic systems. The simplest system to exhibit chaos phenomenon is a one-dimensional discrete-time nonlinear dynamical system. A class of one-dimensional nonlinear maps can produce chaotic sequences whose properties can be designed and analyzed theoretically. In the recent work [2], it is shown that chaos-based spreading in asynchronous DS-CDMA systems is actually optimum in the class of sequences with exponentially vanishing auto-correlations. This means that chaotic sequences can outperform conventional ones in terms of co-channel interference reduction. This is encouraging results for chaos-based communications researchers. Such chaotic sequences with optimum auto-correlations can be generated by several classes of chaotic maps. A simple method of generating chaotic binary sequences with exponentially vanishing auto-correlations have been given in [3].

For practical applications, chaotic sequences are often generated by digital computers in order to guarantee the reproducibility at transmitter and receiver ends. Digital computers have sufficient precision for generating chaotic sequences of reasonable length for practical applications. However, their cost and speed are inferior to conventional sequences which can be generated by simple shift registers. For this problem, we have been trying to generate maximal-period sequences based on one-dimensional maps with finite bits whose shapes are similar to piecewise linear chaotic maps. Some of them are generated by nonlinear feedback shift registers (NFSRs) and their extended versions [4].

This paper is organized as follows. In Section 2, piecewise linear onto maps are introduced. Binary sequences obtained from real-valued sequences generated by such maps have an exponentially vanishing auto-correlation function [3]. Such binary codes can accomplish high performance than conventional spreading sequences for asynchronous DS-CDMA systems. In Section 3, we construct one-to-one maps with finite bits based on piecewise linear chaotic maps. We use maximal-period sequences generated by such maps. That is, we use a minimum precision (the number of bits) for a certain sequence length. However, one-to-one maps cannot always generate maximal-period sequences. So far, we have no method to find maximal-period sequences efficiently. Hence, we have tried to find maximal-period sequence by exhaustive search of all possible plotting according to each type of maps. But, it costs enormous computation time to find maximal-period sequences with long periods. Thus, we give an efficient search algorithm in Section 4.

In Section 5, we investigate bit error rates in asynchronous DS-CDMA systems using our maximal-period sequences by computer simulation. Some comparisons with optimal chaotic codes and conventional spreading codes are also given. Section 6 reports some conclusive remarks and future research directions.

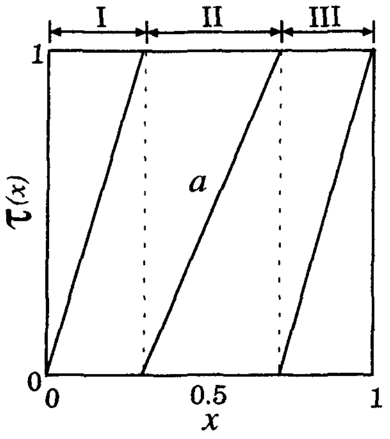

Figure 1: Picewise linear onto map

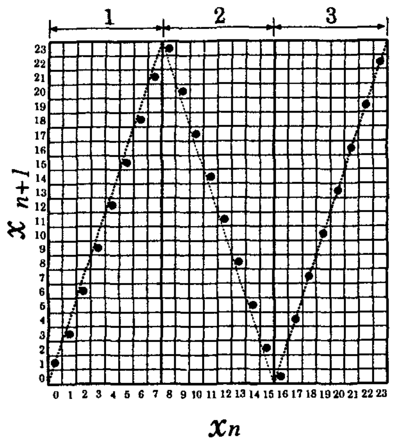

Figure 2: An example of configured maps($a = -3$)

2. Piecewise Linear Onto Map

We employ a class of piecewise linear onto maps(Fig.1) defined by

$$\tau(x) = \begin{cases} \frac{2|a|}{1-|a|}x + 1 & (0 \le x < \frac{1}{2} - \frac{1}{2|a|}) \\ ax - \frac{a-1}{2} & (\frac{1}{2} - \frac{1}{2|a|} \le x < \frac{1}{2} + \frac{1}{2|a|}) \\ \frac{2|a|}{1-|a|}(x-1) & (\frac{1}{2} + \frac{1}{2|a|} \le x \le 1) \end{cases} \quad (1)$$

where $a(|a| > 1)$ is a slope of linear mappings function in the center subinterval. Note that the difference equation $x_{n+1} = \tau(x_n)$ $(n = 0, 1, 2, \cdots)$ generates chaotic real-valued orbits $\{\tau(x_n)\}_{n=0}^{\infty}$ on the unit interval $[0, 1]$ and has the uniform invariant measure. We transform real-valued sequences into binary sequences by the threshold function defined by

$$\Theta_t(x) = \begin{cases} -1 & (x < t) \\ 1 & (x \ge t). \end{cases} \quad (2)$$

The binary sequence $\{\Theta_t(\tau(x)^n)\}_{n=0}^{\infty}$ is called a chaotic binary sequence.

Correlation properties of chaotic binary sequences depend on the chaotic maps and threshold functions. Chaotic binary sequences generated by piecewise linear onto maps and the above threshold function with $t = 0.5$ have an exponentially vanishing auto-correlation function denoted by a^{-l}, where l is the time delay [3]. Thus we can control the auto-correlation properties of chaotic binary sequences by the correlation parameter a. According to [2], $a = -2 - \sqrt{3}$ is the optimum value for asynchronous DS-CDMA systems. Namely, chaotic sequences with auto-correlation $a^{-l}(a = -2-\sqrt{3})$ can outperform conventional spreading sequences such as Gold sequences and Kasami sequences.

3. Realization of Chaotic Sequences with finite bits

For practical applications, chaotic sequences are often generated by digital computers in order to guarantee the reproducibility at transmitter and receiver ends. Digital computers have sufficient precision for generating chaotic sequences of reasonable length for CDMA applications. However, their cost and speed are inferior to conventional spreading sequences most of which can be generated by simple shift registers.

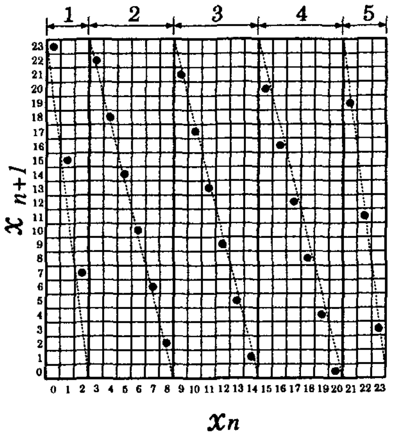

Figure 3: An example of configured maps($a = -4$)

We attempt to generate pseudo-chaotic sequences by configuring one-dimensional maps with finite bits. This approach is very simple in the sense that we don't use real number operations. We only consider generating sequences of integers ($0 \sim N-1$) which can be expressed by $\lceil log_2 N \rceil$ bits. In this paper, we use two piecewise linear chaotic maps with $a = -3$ and $a = -4$ which are close to the optimum parameter $a = -2 - \sqrt{3}$.

Fig.2 shows an example of configured one-to-one maps($N = 24$) based on the chaotic maps with $a = -3$. These maps are configured based on the following rules.

- In the subinterval 2 where the slope of linear mapping functions is -3, x_{n+1} is selected from

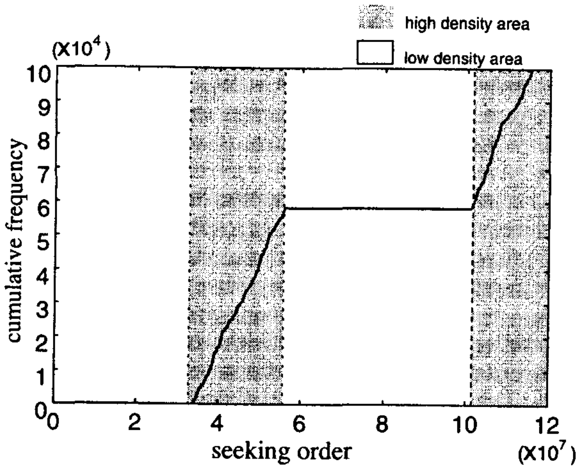

Figure 4: A cumulative distribution of maximal-period-sequence versus the seeking order in our previous algorithm.

$N - 3x_n$, $N - 3x_n - 1$ or $N - 3x_n - 2$.

- In the subinterval 1 and 3 where a slope of linear mapping functions is 3, x_{n+1} is selected from $3x_n$, $3x_n + 1$ or $3x_n + 2$.
- N is restricted to multiples of 6.

Fig.3 shows an example of configured one-to-one maps($N = 24$) based on the chaotic map with $a = -4$. In this case, we use the chaotic map with 5 subintervals in order to make a slope of each subinterval be an integer. This is only for simplification of design. In chaos theory, auto-correlation functions of binary sequences generated by such chaotic maps with 5 subintervals and a threshold 0.5 are also given by a^{-l}, where a is the slope of the center subinterval. Thus these maps are configured base on the following rules.

- In the subinterval 2, 3 and 4 where a slope of linear mapping functions is -4, x_{n+1} is selected from $N-4x_n$, $N-4x_n-1$, $N-4x_n-2$ or $N-4x_n-3$.
- In the subinterval 1 and 5 where a slope of linear mapping functions is -8, x_{n+1} is selected from $N - 8x_n$, $N - 8x_n - 1$, $\cdots$ $N - 8x_n - 7$.
- N is restricted to multiples of 8.

We can generate integer sequences x_n by iterating the map from an initial value x_0(e.g., in Fig.2, $x_0 = 1 \to 3 \to 9 \to \cdots \to 1$). Next, we convert it to binary sequences by threshold $N/2$ which corresponds to a real number 0.5 for the original chaotic map.

4. Search Algorithm

One-to-one maps cannot always generate maximal-period sequences. So far, we have no method to find maximal-period sequences efficiently. Hence, we have tried to find maximal-period sequences by plotting possible mapping points according to each chaotic map in a certain order. But, it costs enormous computation time to find maximal-period sequences with long periods.

Fig.4 shows a cumulative distribution of maximal-period sequences to the seeking order in our previous algorithm, where up to 100,000 maximal-period sequences are found. This figure shows that any maximal-period sequences don't exist till about 3.5 millionth seeking order, but after that, up to about 50,000 maximal-period sequences exist intensively. That is, there are very high densities and very low densities of maximal-period sequences in our previous algorithm.

It is obvious that if we can find a high density area, we can get many maximal-period sequences efficiently. Thus, we propose a new search algorithm as follows. Firstly, we search one maximal-period sequence in a random order. Next, we search other maximal-period sequences in our previous seeking order starting from the order in which the maximal-period sequence exists. By this method, we can avoid long searches in a low density area and can search high density areas intensively.

Tables 1 and 2 show seeking times needed to obtain 1,000 maximal-period sequences in our previous and proposed methods. In these tables , *hit rate*, which is defined as the probability of finding a maximal-period sequences, is also shown. The mark "?" in these tables shows that the seeking times exceeded 0.5 billion and we stopped the computation. From these tables, we can find that the proposed method makes it possible to get maximal-period sequences much more efficiently than

Table 1: Seeking times and hit rate (number of maximal-period sequence=1,000,$a = -3$)

period N	seeking times		hit rate(%)	
	proposed	previous	proposed	previous
48	19,109	7,572	5.2	13.2
120	17,973	2.4×10^8	5.6	4.1×10^{-4}
240	18,882	?	5.3	?
1,032	18,542	?	5.4	?

Table 2: Seeking times and hit rate (number of maximal-period sequence=1,000,$a = -4$)

period N	seeking times		hit rate(%)	
	proposed	previous	proposed	previous
48	13,673	17,199	7.3	5.8
120	29,435	28,797	3.4	3.5
240	32,283	22,245	3.1	4.5
1,032	32,313	?	3.1	?

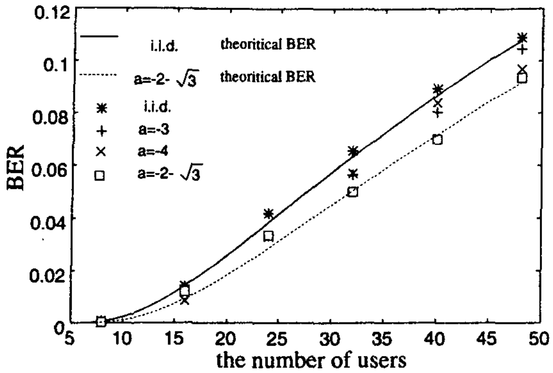

Figure 5: BER ($N = 48$)

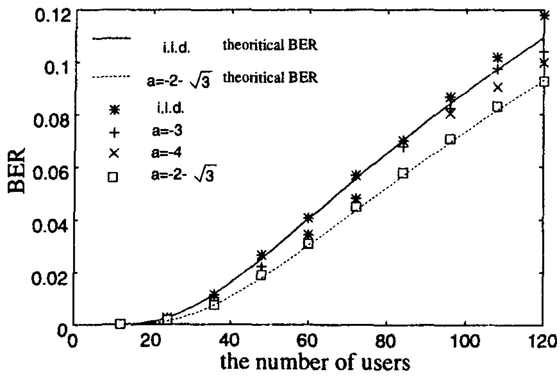

Figure 6: BER($N = 120$)

the previous one for both maps($a = -3, -4$).

5. DS-CDMA Simulation

We investigate bit error rate(BER) in asynchronous DS-CDMA systems using maximal-period sequences as spreading codes by computer simulations. The conditions of these simulations are as follows.

- Sequence length: N=48, 120.
- Number of transmitted information bits: 10,000 bits/user.
- There are random delays between each user.
- No channel noise.

Such a simulation was performed 100 times by changing initial values of random numbers and the average of BER was computed. For comparison, we also use *i.i.d.* binary sequences and optimum chaotic binary sequences with $a = -2 - \sqrt{3}$ both of which are computed by sufficient precision(64-bit floating point operation). Note that *i.i.d.* binary sequences have almost same bit error performances as conventional spreading sequences such as Gold sequences in asynchronous DS-CDMA systems.

Figs.5 and 6 show BER versus the number of active users in asynchronous DS-CDMA systems using each type of sequences. In these figures, solid and broken lines denote the theoretical BER of *i.i.d.* binary sequences and optimal ones, respectively. Such theoretical BER values are in good agreement with simulated ones. Furthermore, we can find that simulated BER values for maximal-period sequences with $a = -3$ and -4 are worse than optimal sequences. We consider that this is because of lack of precision for generating maximal-period sequences. In this case, the necessary number of bits for generating maximal-period sequences is only 7 which is much smaller than 64 bits for generating optimal and *i.i.d.* binary sequences. Finally, it should be noted that the maximal-period sequences outperform *i.i.d.* sequences.

6. Conclusion

We proposed a new search algorithm for finding maximal-period sequences based on some piecewise linear chaotic maps with finite bits. It has been shown that the proposed method can efficiently find maximal-period sequences compared with our previous method. Next, we investigated BER in asynchronous DS-CDMA systems using the maximal-period binary sequences by computer simulation. We found that maximal-period sequences with nagative correlation parameters $a = -3$ and -4 achieve good BER performances which are slightly inferior to the optimal performances but superior to those for *i.i.d.* sequences.

A future work will be directed toward design of generators of maximal-period sequences and their evaluations.

References

[1] D.V.Sarwate and M.B.Pursley, "Crosscorrelation properties of pseudorandom and related sequences", *Proc. IEEE*, Vol.68, No.3, pp.593-619, 1980.

[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] A. Tsuneda, "Design of Chaotic Binary Sequences with Prescribed Auto-Correlation Properties Based on Piecewise Monotonic Onto Maps", *Proc. of 1999 International Symposium on Nonlinear Theory and its Applications*, Vol.2, pp.605-608, 1999.

[4] A. Tsuneda, Y. Kuga, and T. Inoue, "New Maximal-Period Sequences Using Extended Nonlinear Feedback Shift Registers Based on Chaotic Maps", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol.E85-A, no.6, pp.1327-1332, 2002.