


Spreading Sequences with Negative Auto-correlations Generated by LFSRs Based on Chaos Theory of Modulo-2 Added Binary Sequences

Yasunori Miyazaki, Akio Tsuneda, and Takahiro Inoue

Department of Computer Science and Electrical Engineering, Kumamoto University

E-mail: miyaz@st.cs.kumamoto-u.ac.jp, tsuneda@cs.kumamoto-u.ac.jp

2–39–1 Kurokami, Kumamoto 860-8555, Japan
Tel.: +81-96-342-3853, Fax.: +81-96-342-3630

1. Introduction

Linear feedback shift register (LFSR) sequences (e.g., M-sequences, Gold sequences, Kasami sequences) are the most well-known pseudo-random sequences [1] and they are practically used for spreading sequences in direct-sequence code division multiple access (DS/CDMA) systems. As is well known, spreading sequences play an important role in DS/CDMA systems since they dominate the system performance such as bit error rate (BER) [2]. Among many types of spreading sequences, it is especially remarkable that spreading sequences with exponentially vanishing negative auto-correlations can reduce multiple access interference (MAI) in asynchronous DS/CDMA systems compared with the conventional LFSR sequences [3],[4].

Since spreading sequences with exponentially vanishing negative auto-correlations can be generated by one-dimensional chaotic maps, several researchers try to use chaotic sequences with such negative auto-correlations based on some special maps [4]. On the other hand, we have given design methods of binary sequences with negative (but not exponentially vanishing) auto-correlations based on the Bernoulli map and tent maps [5]. We have also shown that binary sequences with negative auto-correlations can be generated by linear/nonlinear feedback shift registers which are a kind of finite-bit realization of the Bernoulli and tent maps. [5],[6].

In this paper, we also design spreading sequences with negative auto-correlations generated by LFSRs, which is based on the chaos theory for the Bernoulli map and modulo-2 added binary sequences. By numerical experiments, we investigate auto-/cross-correlation functions of the proposed sequences.

2. Theoretical Background

A nonlinear difference equation $x_{n+1} = \tau(x_n)$ ($n = 0, 1, 2, \cdots$) can produce a chaotic real-valued sequence $\{\tau^n(x)\}_{n=0}^\infty$ ($\tau^n(\cdot)$ is the $n$-th iteration of the map $\tau(\cdot)$). We can also obtain a binary sequence $\{B(\tau^n(x))\}_{n=0}^\infty$ by a binary function $B(x)(\in \{0, 1\})$. The theoretical auto-correlation of such a binary sequence $\{B(\tau^n(x))\}_{n=0}^\infty$ is defined by

$$C(\ell; B) = E[(2B(x) - 1)(2B(\tau^\ell(x)) - 1)] = \int I(2B(x) - 1)(2B(\tau^\ell(x)) - 1)f^\ell(x)dx$$

under the assumption that $\tau(\cdot)$ has an invariant density function $f^\ell(x)$, where $E[\cdot]$ denotes the expectation and $2B(x) - 1$ implies the transformation $\{0, 1\} \rightarrow \{-1, 1\}$. Assume that $K$ users use chaotic binary sequences $\{B(\tau^n(x(i)))\}_{n=0}^{N-1}$ ($i = 1, 2, \cdots, K$) of length $N$ as its spreading code, 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 [2]

$$\hat{R} = 2N^2 + 4 \sum_{\ell=1}^{N-1} (N - \ell)^2 C(\ell; B)^2 + 2 \sum_{\ell=1}^{N-1} (N - \ell)(N - \ell + 1)C(\ell; B)C(\ell - 1; B).$$

Furthermore, define a normalized AIP by

$$R = \lim_{N \rightarrow \infty} \frac{\hat{R}}{2N^2}.\quad (3)$$

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

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

$$R = \frac{\lambda^2 + \lambda + 1}{1 - \lambda^2}$$

which takes the minimum value $\frac{\sqrt{3}}{2}$ when $\lambda = -2 + \sqrt{3}$ [3],[4]. Thus such sequences have smaller AIPs than uncorrelated sequences with $R = 1$. 

541
Next consider the sequences whose auto-correlation function is given by
\[ C(\ell; B) = \begin{cases} 
1 & (\ell = 0) \\
\varepsilon & (\ell = 1) \\
0 & (\ell \geq 2),
\end{cases} \]  
(5)

where |\varepsilon| < 1. In this case, the calculation of AIP is much easier than the case \( C(\ell; B) = \lambda^\ell \) and we have
\[ \hat{r} = 2N^2 + 4(N-1)^2\varepsilon^2 + 2N(N-1)\varepsilon \]  
(6)
\[ R = 2\varepsilon^2 + \varepsilon + 1 \]  
(7)

which take the minimum values \( \frac{7N^2+1}{4} \) and \( \frac{7}{8} \) when \( \varepsilon = -\frac{1}{2} \) respectively. These minimum values are slightly larger than the case \( C(\ell; B) = \lambda^\ell \) with \( \lambda = -2 + \sqrt{3} \) but the differences are quite small. Of course, the sequences of this case (\( \varepsilon = -\frac{1}{2} \)) also outperform the uncorrelated sequences with \( R = 1 \).

Now consider a new type of binary sequence \( \{B_n\}_{n=0}^{\infty} \) generated by modulo-2 addition of two chaotic sequences \( \{B_1(\tau^n(x))\}_{n=0}^{\infty} \) and \( \{B_2(\tau^n(y))\}_{n=0}^{\infty} \), that is, \( B_n = B_1(\tau^n(x)) \oplus B_2(\tau^n(y)) \). Assume \( x \) and \( y \) are statistically independent of each other and \( E[B_1(\tau^n(x))] = E[B_2(\tau^n(y))] = \frac{1}{2} \). The auto-correlation function of \( B_n \) is given by [7]
\[ C(\ell; B_n) = C(\ell; B_1(\tau^n(x)))C(\ell; B_2(\tau^n(y))). \]  
(8)

Here we consider the Bernoulli map \( \tau_B(x) \) defined by
\[ \tau_B(x) = \begin{cases} 
2x & (0 \leq x < \frac{1}{2}) \\
2x-1 & (\frac{1}{2} \leq x \leq 1)
\end{cases} \]  
(9)

and two binary function \( B_1(x) \) and \( B_2(x) \) defined by
\[ \begin{cases} 
B_1(x) = \Theta_1(x) - \Theta_2(x) + \Theta_3(x) - \Theta_4(x) + \Theta_5(x), \\
B_2(x) = \Theta_1(x) - \Theta_2(x) + \Theta_3(x) \end{cases} \]  
(10)

where \( \Theta_i(x) \) is a threshold function defined by
\[ \Theta_i(x) = \begin{cases} 
0 & (x < t) \\
1 & (x \geq t). 
\end{cases} \]  
(11)

Since the Bernoulli map \( \tau_B(x) \) has the uniform invariant density function \( f^*(x) = 1 \), we have \( E[B_i(\tau_B^n(x))] = \frac{1}{2} \) \( (i = 1, 2) \). We also have the following theoretical results.
\[ C(\ell; B_1(\tau_B^n(x))) = \begin{cases} 
1 & (\ell = 0) \\
-\frac{1}{4} & (\ell = 1) \\
\frac{1}{4} & (\ell = 2) \\
0 & (\ell \geq 3)
\end{cases}, \]  
(12)
\[ C(\ell; B_2(\tau_B^n(x))) = \begin{cases} 
1 & (\ell = 0) \\
\frac{1}{4} & (\ell = 1) \\
\frac{1}{4} & (\ell = 2) \\
0 & (\ell \geq 3).
\end{cases} \]  
(13)

We consider a binary sequence \( \{B_n\}_{n=0}^{\infty} \) obtained by modulo-2 addition of \( \{B_1(\tau_B^n(x))\}_{n=0}^{\infty} \) and \( \{B_2(\tau_B^n(y))\}_{n=0}^{\infty} \), that is,
\[ B_n = B_1(\tau_B^n(x)) \oplus B_2(\tau_B^n(y)). \]  
(14)

From eqs. (8), (12), and (13), we have
\[ C(\ell; B_n) = \begin{cases} 
1 & (\ell = 0) \\
-\frac{1}{4} & (\ell = 1) \\
\frac{1}{16} & (\ell = 2) \\
0 & (\ell \geq 3).
\end{cases} \]  
(15)

In asynchronous DS/CDMA system, the auto-correlation property of eq.(15) (which gives \( R = \frac{11}{128} \)) is slightly inferior to the exponentially vanishing property with the optimum parameter \( \lambda = -2 + \sqrt{3} \) (which gives \( R = \frac{\sqrt{3}}{2} \) in eq.(4)). However, it is slightly better than the property of eq.(5) giving \( R = \frac{1}{4} \) when \( \varepsilon = -\frac{1}{2} \).

3. Proposed Sequence Generator

In this study, we design spreading sequences with negative auto-correlations to be generated by using LFSRs based on the theoretical results given in the previous section. Fig.1 shows the conventional Gold sequence generator which is based on modulo-2 addition of preferred pair of M-sequences generated by two k-stage LFSRs. It is noteworthy that LFSRs can be regarded as a finite-bit approximation of the Bernoulli map [8].

Thus, similar to the configuration of the Gold sequence generator in Fig.1, the proposed sequence generator is shown in Fig.2. In the proposed generator, each LFSR has an additional combinational logic circuit with 3 inputs which corresponds to a binary function \( B_1(x) \) or \( B_2(x) \) in eq.(10). Namely, the two additional logic functions are given by
\[ f_1(a_0, a_1, a_2) = \begin{cases} 
1 & a_0a_1a_2 \in \{001, 100, 101, 111\} \\
0 & \text{otherwise},
\end{cases} \]  
(16)
\[ f_2(a_0', a_1', a_2') = \begin{cases} 
1 & a_0'a_1'a_2' \in \{011, 101, 110, 111\} \\
0 & \text{otherwise}.
\end{cases} \]  
(17)

These logic functions are finite-bit versions of eq.(10).

By changing the initial state of one register (except all-zero state), we can obtain \( 2^k - 1 \) different binary sequences (called a family) by the proposed generator, which is similar to the Gold sequence generator. Note that a family of Gold sequences consists of \( 2^k + 1 \) sequences including the original two M-sequences [1], while we cannot use the original two sequences before modulo-2 addition in our proposed generator.

4. Numerical Experiments

We performed some numerical experiments concerning statistical properties of sequences generated by the proposed generator. Here we generate the proposed sequences using (a) two same M-sequences, (b) preferred...
sequences. The distributions of cross-correlation values are shown in each figure. The distributions of cross-correlation values are averaged for 63 (or 62) sequences of the sequences. For comparison, the auto-correlation functions of sequences generated by modulo-2 addition of the original M-sequences are also shown in each figure (i.e., the case (b) denotes Gold sequences). We find that the proposed sequences have a negative auto-correlation value at the delay time 1 and a positive auto-correlation value at the time delay 2, which are almost equal to the theoretical ones. Especially, the auto-correlation function of (b) is in good agreement with the theoretical function given by eq.(15).

On the other hand, Fig.4 shows the distributions of the cross-correlation values of the proposed sequences for $k = 6$, where all the possible pairs in a family of the 63 (or 62) sequences are taken into account. The cross-correlations of sequences generated by modulo-2 addition of the original M-sequences are also shown in each figure. The distributions of cross-correlation values are Gaussian-like distributions with 0 mean and their maximum values are slightly greater than those of Gold sequences.

5. Concluding Remarks

We have designed spreading sequences with negative auto-correlations generated by LFSRs, which is based on the chaos theory for the Bernoulli map and modulo-2 added binary sequences. Numerical experiments showed that the auto-correlation value of the proposed binary sequences at the delay time 1 and 2 are almost equal to the theoretical values $-0.25$ and $0.0625$, respectively. On the other hand, the distributions of cross-correlation values are similar to the Gaussian distribution with 0 mean and their maximum values are slightly greater than those of Gold sequences.

According to the theoretical analysis of asynchronous DS/CDMA systems, the proposed sequences are expected to reduce the BER compared with the conventional LFSR sequences. Simulations of asynchronous DS/CDMA systems using the proposed sequences are left to future studies.

References


Figure 3. Average auto-correlation functions of the proposed sequences generated by (a) two same M-sequences, (b) preferred pair of M-sequences, and (c) non-preferred pair of M-sequences, where $k = 6$.

Figure 4. Distributions of cross-correlation values of the proposed sequences generated by (a) two same M-sequences, (b) preferred pair of M-sequences, and (c) non-preferred pair of M-sequences, where $k = 6$. 