

New chaotic binary sequences with good correlation property using logistic maps

Chikhaoui Fatima, Djebbari Ali

Telecommunications and Digital Signal Processing Laboratory, Djillali Liabes University, Sidi Bel-Abbes
Algeria

Abstract: In this paper, schemes for generating binary sequences from logistic maps are proposed. Using new methods, several binary sequences with the same length can be generated directly by assuming different initial conditions to logistic maps. A comparison between conventional sequences (maximum length sequences, Gold sequences) and proposed sequences has been established, and demonstrate that our sequences are comparable and even superior to conventional sequences in several keys aspects, and they can be used as spreading sequences.

Keywords- Conventional sequences, correlation function, Direct Sequence Code Division Multiple Access (DS-CDMA), logistic maps.

I. Introduction

Properties of chaotic sequences such as: sensitivity to initial conditions, flexibility of the length of sequences (sequences are not restricted in length), the multiple access capability (unlimited number of sequences of a given length), good correlation properties and difficulty of interception [1, 2] make them potential candidates for applications of spreading spectrum. Many researchers are interested in the generation of binary sequences [3]-[5] and their use in DS-CDMA system. In [3] a quantization and encoding block is used to generate binary sequences from open flow coupled map lattices, synchronization of chaotic sequences generator in the receiver is driven by use of a sequence from the transmitter generator. Moreover, in [4] binary sequences are obtained by two procedures: Conversion into integer then into binary sequences, transmitter and receiver generators are realized as the same way. However, in [5] binary sequences are generated from chaotic sequences using a multiplier, an integer part, modulo operation and at the last part a block of binary conversion.

Many problems are encountered in the existing techniques: synchronization between transmitter and receiver generators [3], complexity of generator (several procedures to be made); the number of bits of the source information must be known [4], several blocks are needed, in addition, sequences generated from different initial conditions (for different users) have not the same length[5]. However, the two proposed methods uses simple construction techniques compared to the existing methods [3]-[5], and binary sequences generated from different initial conditions have the same length.

This paper proposes two schemes for generating chaotic binary sequences using logistic maps. The paper is organized as follows: Section 2 presents logistic maps and their properties. In section 3 we present our proposed methods. Correlation properties of proposed sequences are discussed in section 4. Section 5 presents an overview of conventional sequences and their limits. Comparison between our proposed sequences and conventional sequences is given in section 6. Conclusion is drawn in last section.

II. Logistic maps

Chaotic sequences are generated using discrete chaotic functions. One of the most common utilizing is the logistic maps that can be given by the two following equations [6, 7]:

$$x_{n+1} = r x_n (1 - x_n) \quad (1)$$

$$x_{n+1} = 1 - 2 x_n^2 \quad (2)$$

In equation (1), $x_n \in]0, 1[$ ($n=0, 1, \dots$), and $0 < r \leq 4$ is called the bifurcation parameter, for $r \in]3.57, 4[$ the sequence generated from (1) is chaotic [6]. In equation (2), $x_n \in]-1, 1[$ ($n=0, 1, \dots$).

The concept of sensitivity of chaotic maps given by equations (1) and (2) to initial conditions can be illustrated giving two close values of initial value x_0 , after a few iterations, the two sequences generated by each equation will look completely uncorrelated. Fig.1 and Fig.2 illustrates this point (30 iterations are done).

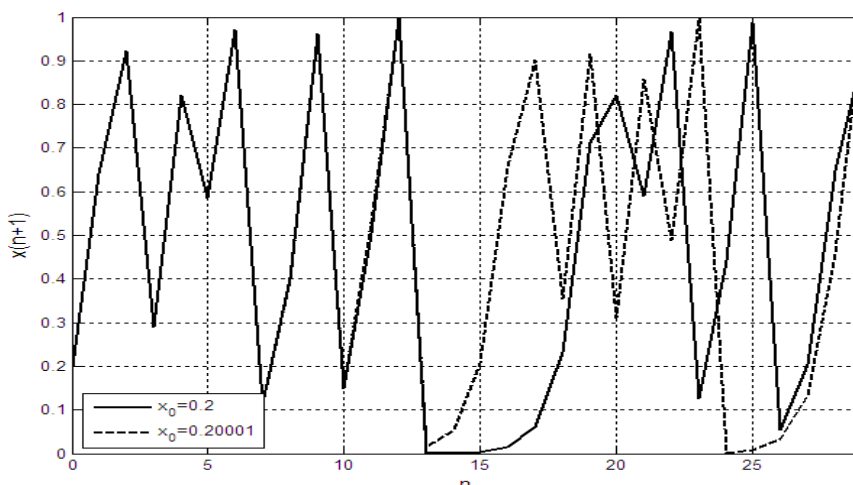


Fig.1 Sequences generated by equation (1) for two initial conditions

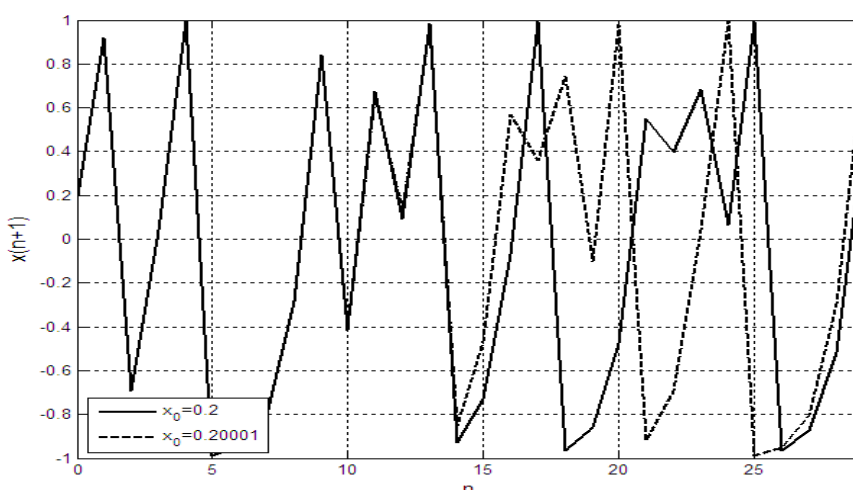


Fig.2 Sequences generated by equation (2) for two initial conditions

III. Proposed methods

In order to generate binary sequences derived from logistic maps and to achieve multi-user communication in DS-CDMA system, new schemes are proposed. For each logistic map given by either equation (1) or equation (2), binary sequences are generated by using the models shown in Fig.3 and Fig.4.

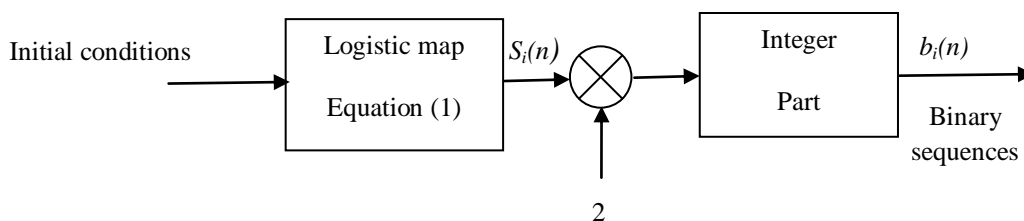


Fig.3 Block diagram of the first binary sequences generator

The generator is governed by the following equation:

$$b_i(n) = \lfloor 2 \times S_i(n) \rfloor, i = 1, 2, \dots, K \tag{3}$$

Where K is the number of coupled maps (number of users), $S_i(n)$ is the chaotic sequence generated from the i^{th} map, and $\lfloor \quad \rfloor$ is the integer part.

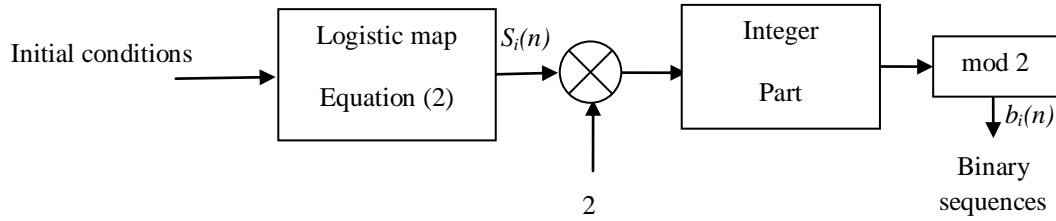


Fig.4 Block diagram of the second binary sequences generator

This generator is governed by equation (4):

$$b_i(n) = \lfloor 2 \times S_i(n) \rfloor \bmod 2 \tag{4}$$

IV. The correlation functions of proposed sequences

One of the basic properties of spreading sequences is that of auto- and cross-correlation functions, in this section; we propose to discuss these properties.

IV.1. Auto-correlation function

For a given binary sequence $b_i(n)$ with length L, normalized auto-correlation function is defined by:

$$R_{AC}(\tau) = \frac{1}{L} \sum_{n=0}^{L-1} b_i(n) b_i(n+\tau), \quad 0 \leq \tau \leq L-1 \tag{5}$$

Auto-correlation function of the spreading sequences must have values as small as possible for $\tau \neq 0$. Proposed sequences verify this condition well especially when the length of sequence is important.

Fig.5 and Fig.6 shows auto-correlation functions of our proposed sequences for $L=1500, x_0=0.22$.

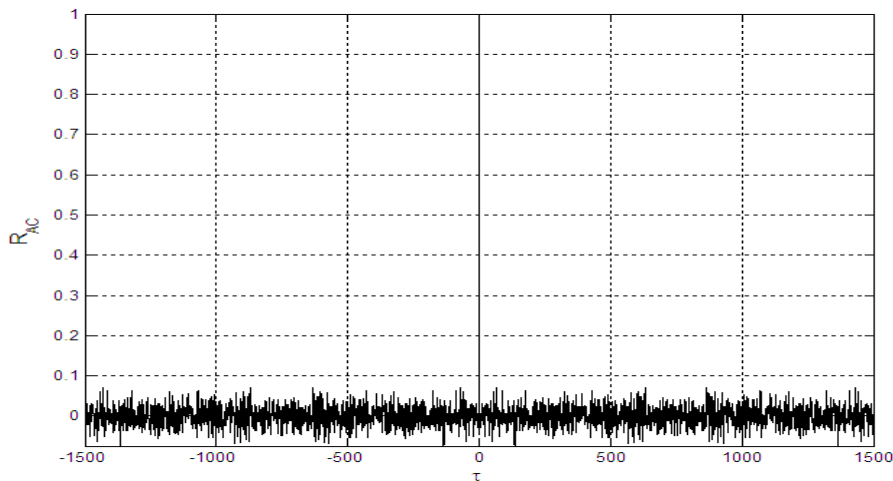


Fig.5 Auto-correlation of binary sequences, equation (3), $r=4, L=1500$

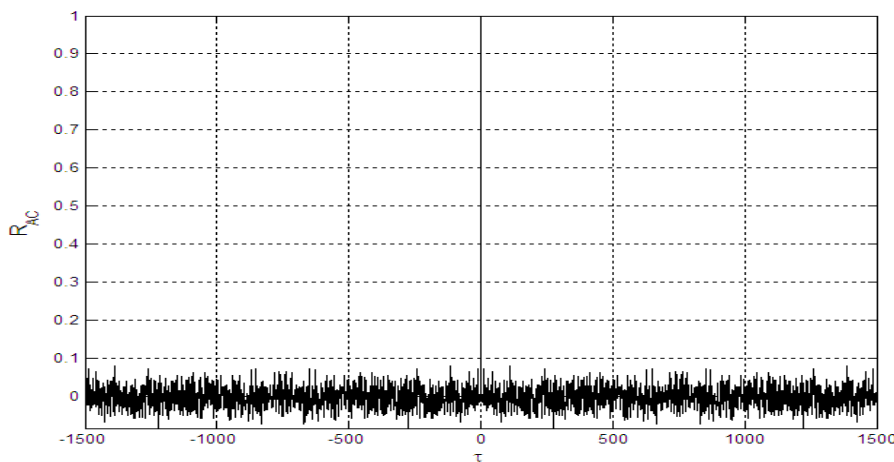


Fig.6 Auto-correlation of binary sequences, equation (4), $L=1500$

IV.2. Cross-correlation function

Consider two binary sequences $b_i(n)$ and $b_j(n)$ with the same length L , normalized cross-correlation function is given as follows:

$$R_{CC}(\tau) = \frac{1}{L} \sum_{n=0}^{L-1} b_i(n) b_j(n+\tau), \quad 0 \leq \tau \leq L-1 \quad (6)$$

Values of cross-correlation function must be as small as possible for all values of τ . For chaotic sequences, values of cross-correlation tend towards zero value, in Fig.7 and Fig.8, we show these values for our proposed binary sequences with length 1500, initial conditions are $x_0=0.1$ and $x_0=0.2$.

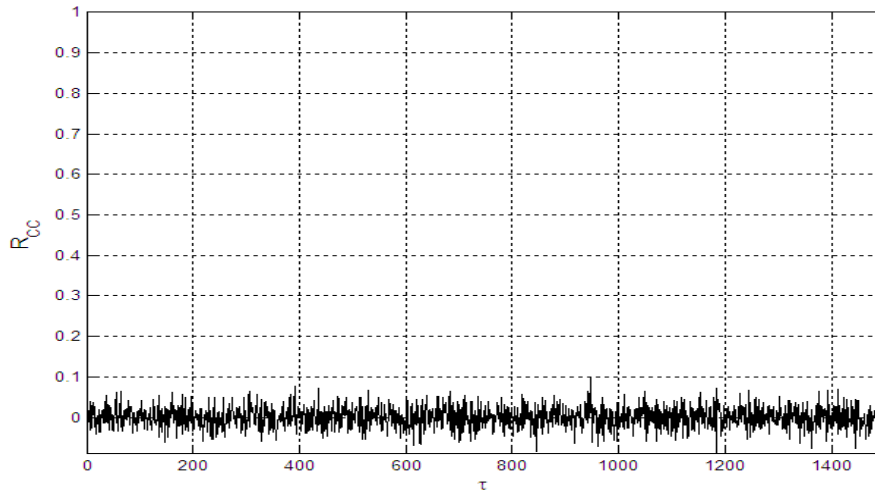


Fig.7 Cross-correlation of binary sequences, equation (3), $r=4$, $L=1500$

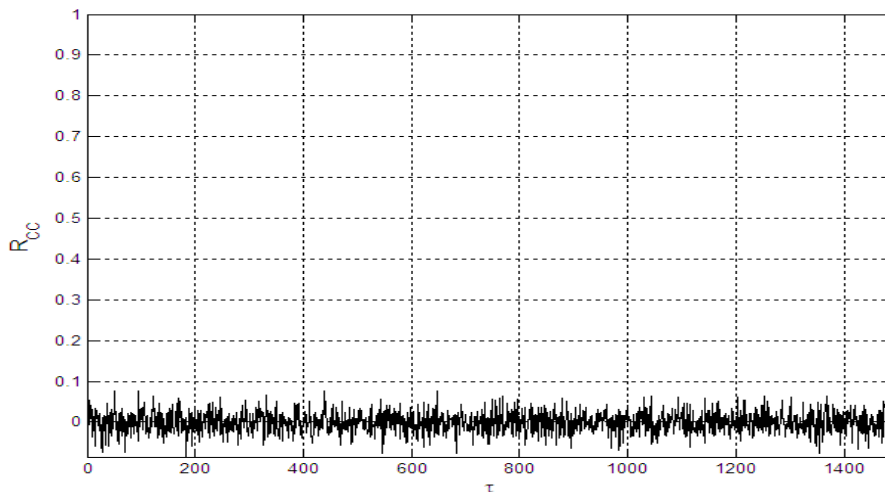


Fig.8 Cross-correlation of binary sequences, equation (4), $L=1500$

V. Conventional sequences

V.1. Maximum length sequences

m-sequences for short, they are by far the most popular spreading sequences generated by linear feedback shift registers [8]. For a given shift register with length n , length of m-sequence generated is $L=2^n-1$. The normalized auto-correlation function of these sequences is $-1/L$ for all delays away from the origin. While, this value approaches zero as the length of sequences increase, large spikes can be found in their cross-correlation functions [9]. Another undesirable property of m-sequences is that they are restricted in number (for a given length). For example, for $L=127$, there are only 18, and for $L=255$, there are only 16 possible different sequences for use.

V.2. Gold sequences

To overcome the problem of large spikes of cross-correlation functions found in m-sequences, Gold sequences are used [10]. They are constructed using preferred pairs of m-sequences [9].

Given preferred pairs of length L, the number of Gold sequences that can be generated is L+2. Cross-correlation function of Gold sequences is controlled for all sequences and is defined by three values given by:

$$R_{CC}(\tau) = \begin{cases} -1/L \\ -t(n)/L \\ (t(n)-2)/L \end{cases} \quad (7)$$

Where $t(n)$ is given by:

$$t(n) = \begin{cases} 2^{(n+2)/2} + 1 & n \text{ even} \\ 2^{(n+1)/2} + 1 & n \text{ odd} \end{cases} \quad (8)$$

Auto-correlation function of Gold sequences takes values of cross-correlation function except at zero delay [9] (So the auto-correlation function will be worse than that of m-sequences). A shortcoming of Gold sequences is that they can be obtained only for well-defined lengths [10].

VI. Sequences comparison

In the previous section, we have noted that conventional sequences are limited in several aspects: complexity of construction, length of sequences, and number of possible sequences.

Merit indicators of correlation function for DS CDMA system can be a maximum value of auto-correlation for $\tau \neq 0$ and a maximum value of cross-correlation for a set of sequences.

We propose in this section to analyze these values for different lengths of our binary sequences and conventional sequences using as criteria the maximum values of correlation functions given in [11]:

$$M_{AC} = \max_i \max_{\tau \neq 0} |R_{AC}(\tau)| \quad (9)$$

$$M_{CC} = \max_{i \neq j} \max_{\tau} |R_{CC}(\tau)| \quad (10)$$

Values of M_{AC} and M_{CC} are listed for various lengths of chaotic binary, m- and Gold sequences in TABLES (1) and (2) respectively.

Table.1 Maximum auto-correlation of chaotic binary, m- and Gold sequences

Length of sequences	M_{AC}			
	Chaotic binary sequences		m-sequences	Gold sequences
	Equation (3)	Equation (4)		
7	0.1429	0.1429	0.1429	0.7143
15	0.0667	0.0667	0.0667	*
31	0.0968	0.0968	0.0323	0.2903
63	0.1429	0.1111	0.0159	0.2698
127	0.1181	0.1181	0.0079	0.1339
255	0.1059	0.0980	0.0039	*

* no defined

Table.2 Maximum cross-correlation of chaotic binary, m- and Gold sequences

Length of sequences	M_{CC}			
	Chaotic binary sequences		m-sequences	Gold sequences
	Equation (3)	Equation (4)		
7	0.4286	0.1429	0.7143	0.7143
15	0.2000	0.3333	0.6000	*
31	0.2258	0.2903	0.3548	0.2903
63	0.2381	0.2381	0.3651	0.2698
127	0.1339	0.1339	0.3228	0.1339
255	0.1294	0.1294	0.3725	*

* no defined

For chaotic binary sequences, there is an infinite set of initial conditions and hence sequences available. To perform the correlation calculations, for each length L , M_{AC} and M_{CC} are calculated for different initial conditions which are taken with an accuracy of 10^{-5} . We can see from TABLES (1) and (2) that chaotic binary sequences offer better performances compared to those obtained with conventional sequences, namely for cross-correlation function which is necessary in multi-user systems. In terms of auto-correlation, our chaotic binary sequences present better values compared to Gold sequences but remains higher than those obtained by m-sequences. In addition to the advantages of improved correlation properties, the proposed methods provide other advantages over conventional sequences: a) simplicity of construction b) large flexibility (number of users is independent of length) in choosing the number of users and c) code length (free choice of code length).

VII. Conclusion

Purpose of this paper is the generation of chaotic binary sequences for use in DS-CDMA system. New sequences have been constructed in a simple way using simplest chaotic functions named logistic maps. Sequences generated with proposed schemes have the same length (length is independent of initial conditions) for all initial conditions.

Chaotic binary sequences outperform conventional sequences in several keys aspects: complexity of generation, flexibility in choosing the length of sequence and multiple access capability.

Correlation functions of the proposed sequences show that these sequences are found to be suitable for use as spreading sequences in DS-CDMA system.

References

- [1] G. Heidari-Bateni and C.D. McGillem, Chaotic Sequences for Spread Spectrum: An Alternative to PN-sequences, *Proc. IEEE International Conference on Selected Topics in Wireless Communications*, Vancouver, B.C, Canada, 1992, 437-440.
- [2] G. Heidari-Bateni and C.D. McGillem, A Chaotic Direct-Sequence Spread Spectrum Communication System, *IEEE Trans. On Communications*, 42(2/3/4), 1994, 1524-1527.
- [3] H. Saigui, Z. Yong, H. Jiandong and B. Liu, A synchronous CDMA system using discrete coupled-chaotic sequence, *Proc. IEEE South-eastcon '96*, 1996, 484-487.
- [4] Xingang Wang, Meng Zhan, Xiaofeng Gong, Choy Heng Lai and Ying-Cheng Lai, Spread spectrum communication using binary spatiotemporal chaotic codes, *Phys. Lett. A*, 2005, 334, 30-36.
- [5] Mahalinga V. Mandi, R. Murali and K.N. Haribhat, Chaotic functions for generating binary sequences and their suitability in multiple access, *Proc. IEEE International Conference on Communication Technology*, 2006, 1-4.
- [6] Tien-Yien. Li and James.A. Yorke, Period three implies chaos, *JSTOR*, 82(10), 1975, 985-992.
- [7] S.S. Rao and S.P. Howard, Correlation performance of chaotic signals in spread spectrum systems, *Proc. IEEE, Digital Signal Processing Workshop*, 1996, 506-509.
- [8] N. Zierler, Linear recurring sequences, *Journal of the Society for Industrial and Applied Mathematics*, 7(1), 1959, 31-48.
- [9] D.V. Sarwate, M.B. Pursley, Cross-correlation Properties of Pseudorandom and Related Sequences, *Proc. IEEE Digital Signal Processing Workshop*, 68(5), 1980, 593-619.
- [10] R. Gold, Optimal binary sequences for spread spectrum multiplexing, *IEEE Trans, on Information Theory*, 13, 1967, 619-621.
- [11] D. Sandoval-Morantes and D. Munoz-Rodrigues, Chaotic sequences for multiple access, *Electronics Letters*, 34(3), 1998, 235-237.