Spreading Sequences Generated Using Asymmetrical Integer-Number Maps

Vladimír ŠEBESTA

Dept. of Radio Electronics, Brno University of Technology, Purkyňova 118, 612 00 Brno, Czech Republic

sebesta@ feec.vutbr.cz

Abstract. *Chaotic sequences produced by piecewise linear maps can be transformed to binary sequences. The binary sequences are optimal for the asynchronous DS/CDMA systems in case of certain shapes of the maps. This paper is devoted to the one-to-one integer-number maps derived from the suitable asymmetrical piecewise linear maps. Such maps give periodic integer-number sequences, which can be transformed to the binary sequences. The binary sequences produced via proposed modified integer-number maps are perfectly balanced and embody good autocorrelation and crosscorrelation properties. The number of different binary sequences is sizable. The sequences are suitable as spreading sequences in DS/CDMA systems.*

Keywords

Chaotic map, integer-number map, binary spreading sequence.

1. Introduction

The direct-sequence (DS) code-division multiple-access (CDMA) has many desirable features such as robustness to fading and narrow-band interference suppression. In DS/CDMA systems, the bandwidth of the input signal is spread by a spreading sequence with a much higher rate.

The main requirements to the set of the spreading sequences are δ-like autocorrelation function, zero cross-correlation function and ideal balance properties. Many sets of the spreading sequences have been developed. For example *m*-sequences, Gold sequences, Kasami sequences, fixed- and variable-length orthogonal codes. Their properties approach to the ideal ones more or less. This paper is devoted to the chaotic spreading sequences.

Most of known chaotic systems are continuous-time chaotic systems [1]. Discrete-time chaotic systems and signals are introduced and analyzed, too. These systems are usually described using 1-D chaotic maps [2] and are able to create sequences of real numbers. A few publications are devoted to the discretized chaotic maps, e.g. to the integer-number maps [3]. The discretized maps cannot produce real chaos. The generated sequences are called pseudo-chaos, digital chaos, finite-state chaos or discrete-time and discrete-value chaos. Every sequence is periodic regardless of the initial value if the digital map is one-to-one. One method for obtaining a digital one-to-one map has been described in [4]. In this article we will utilize a similar method.

A discrete-time chaotic sequence can be transformed to a binary sequence [5]. It enables various applications in communications and cryptography. Statistical properties of the binary sequences have been studied [6].

Utilization of the chaotic binary sequences as the spreading sequences was analyzed and studied [7]. Convenience of the pseudo chaotic sequence in comparison with the pseudo-random sequence for the asynchronous DS/CDMA system has been proved and experimentally verified [8]. Recently, maps with a tunable autocorrelation of the binary sequence have been proposed [9]. After that, maximal-period sequences with negative autocorrelation have been presented [10], [11]. Some restrictions to the map parameter were used to keep computational complexity reasonable. The method proposed in this paper is based on the different technique of quantization [3] and provides substantially wider set of sequences.

The aim of this paper is to examine the integer-number one-to-one map as the binary spreading sequence generator. We will define and study the centrally asymmetrical maps. The maps can be used to obtain binary sequences with good autocorrelation and cross correlation characteristics. Sec. 2 of this paper provides theoretical background. Previously, we have proposed and tested classification and identification of the integer-number maps [12]. In Sec. 3 we will describe how the identification will allow modifying the map and achieving the constant length of the sequence. Fine tuning the piecewise-linear continuous map changes the associated integer-number map and the correlation properties of the binary sequence. In Sec. 4 we will describe how tuning enables to pick out sequences of desired properties.

2. Theory

2.1 Continuous Map and Integer Number Map

Let us suppose the chaotic sequence $x_{c,n}$ is described in the iterative form:

$$x_{c,n+1} = \tau_c(x_{c,n}), \quad n = 0, 1, 2, \tag{1}$$

where $\tau_c(x_{c,n})$ is a 1-D chaotic map, τ_c: $X_c \rightarrow X_c$ and $x_{c,n}$ is a value of the chaotic sequence in time n. The initial value $x_{c,0}$ is assumed to be a nonpathological. Suppose, the set X_c is the interval [0, 1].

The chaotic sequence $x_{c,n}$, n=0,1,2,… is defined by the two factors:
a) the map configuration, i.e. mapping τ_c: $X_c \rightarrow X_c$,
b) the initial value $x_{c,0}$ of the sequence.

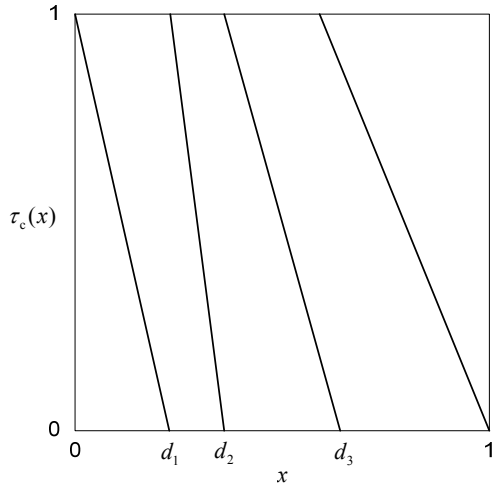

Fig. 1. Piecewise linear map.

The binary sequence $b_{c,n}$ can serve as the spreading sequence. For maps with the equidistributivity property in the interval [0, 1], the next simple rule can be used for quantization:

$$b_{c,n} = \begin{cases} -1 & \text{for} \quad x_{c,n} < 0.5 \quad \text{and} \\ 1 & \text{for} \quad x_{c,n} \geq 0.5 \end{cases}. \tag{2}$$

The integer-number sequence x_n can be described in an iterative form:

$$x_{n+1} = \tau_d(x_n), \quad n = 0, 1, 2, ... \tag{3}$$

where $\tau_d(x_n)$ is a 1-D integer-number map τ_d:$X_d \rightarrow X_d$ and x_n is a value of the sequence x_n in time n. The set X_d is the set $\{1, 2, 3, ... , N\}$, where $N = 2^{N_b}$ and N_b is the number of binary digits used for binary representation of the elements of the set X_d.

The map τ_d can be obtained using quantization of the piece-wise continuous chaotic map τ_c [4]. Then, the sequence x_n is usually nearly chaotic and can be called the pseudo-chaos. For small n and big N we can write

$$x_{c,n} \cong \frac{x_n - 0.5}{N}. \tag{4}$$

The binary sequence b_n can be determined via quantization of the discrete-time pseudo-chaotic signal x_n :

$$b_n = \begin{cases} -1 & \text{for} \quad x_n < H \quad \text{and} \\ 1 & \text{for} \quad x_n \geq H \end{cases} \tag{5}$$

where H is a suitable threshold.

2.2 Optimal Chaotic Maps

A certain class of the chaotic maps allows achieving the next autocovariance function of the binary sequence [9]:

$$C_o(m) = \frac{1}{(-2-\sqrt{3})^m} \tag{6}$$

where m is the delay. The generated binary sequence is then optimal as the spreading sequence for the asynchronous DS/CDMA systems in terms of minimization of average co-channel interference. The chaotic map has to be fully stretching piecewise-linear map. The slope $\tau_c'(x)$ of the map has to be equal to -2-√3 and $\tau_c(x)$ has to be equal to 0.5 for x=0.5.

An example of such map is drawn in Fig. 1. A partition such that $0=d_0<d_1<d_2<d_3<d_4=1$ has been used, where $d_3-d_2=(2+\sqrt{3})^{-1}$ and $d_2=1-d_3$. Parameter d_1 is a tuned parameter of the map. Thanks to it, different maps can be made. An example of the associated integer-number map is shown in Fig. 2 using circles.

2.3 Centrally Asymmetrical Maps

Definition 1: Any chaotic map, τ_c: $X_c \rightarrow X_c$ which satisfies the condition

$$\tau_c(x_c) = 1 - \tau_c(1 - x_c) \tag{7}$$

for all $x_c \in X_c$ is called the centrally symmetrical map.

All other maps are centrally asymmetrical maps. The map in Fig. 1. is asymmetrical.

A discrete integer-number one-to-one map derived from asymmetrical piecewise-linear chaotic map produces several disjoint periodic subsequences or only one periodic sequence. Every subsequence has period less then $N = 2^{N_b}$. The sum of periods of all subsequences is equal to $N = 2^{N_b}$.

2.4 Correlation of the Pseudo-Chaotic Sequences

An autocovariance function of the pseudo-chaotic binary sequence b_n is even and periodic. It is given by

$$C(m) = \frac{1}{M}\sum_{n=0}^{M-1} b_n b_{n+m} \tag{8}$$

where M is the period of the sequence, m is the delay.

The experimental autocovariance function has been compared with the optimal function $C_o(m)$ defined by Eq. (6). The difference between $C(m)$ and $C_o(m)$ was evaluated using the quantity

$$RMS = \sqrt{\frac{2}{M}\sum_{m=0}^{0.5M-1}\left[C(m)-C_o(m)\right]^2}\,. \tag{9}$$

Another possible quantity for evaluation of the quality is the absolute value of the difference $C(m)$ - $C_o(m)$:

$$MAE = \max_{m\in\langle 0,\ 0.5M-1\rangle}\left[\left|C(m)-C_o(m)\right|\right]. \tag{10}$$

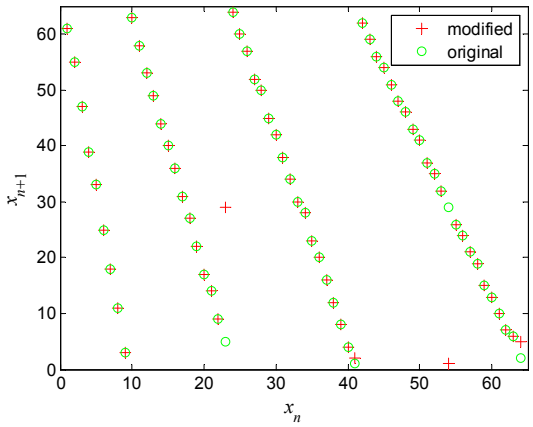

Fig. 2. An original integer-number map and the modified map. N_b=6.

The crosscovariance between two pseudo-chaotic binary sequences $b_i(n)$ and $b_j(n)$ has been tested using the quantity

$$RMSc = \sqrt{\frac{1}{M}\sum_{m=0}^{M-1}\left[C_{ij}(m)\right]^2} \tag{11}$$

and using maximum of the absolute value of $C_{ij}(m)$

$$MAEc = \max_{m\in\langle 0,\ M-1\rangle}\left[\left|C_{ij}(m)\right|\right] \tag{12}$$

where M is the period of the sequences and

$$C_{ij}(m) = \frac{1}{M}\sum_{n=0}^{M-1} b_{i,n}\, b_{j,n+m} \tag{13}$$

is the crosscovariance.

3. Designing the Map

The proposed procedure consists of the following steps:

a) Creating the asymmetric chaotic map according to paragraph 2.2. An example of the map is shown in Fig. 1.

b) Developing the integer-number one-to-one map. Such map is shown in Fig. 2 via circles.

c) Identification of its all periodic subsequences.

d) Concatenating all periodic subsequences to achieve one periodic sequence with $N = 2^{N_b}$ elements in the period.

e) Forming the modified map from the sequence. This map is shown in Fig. 2 using pluses.

f) Quantization of the sequence to achieve binary sequence.

The quantity $M = N$ is even. Quantization level H is simply equal to $0.5N$ and the binary sequence is perfectly balanced. Similarly, the thresholds 0.25 N, 0.5 N and 0.75 N are the optimal ones for creating a balanced four-state sequence. It is needed in the case of the complex spreading.

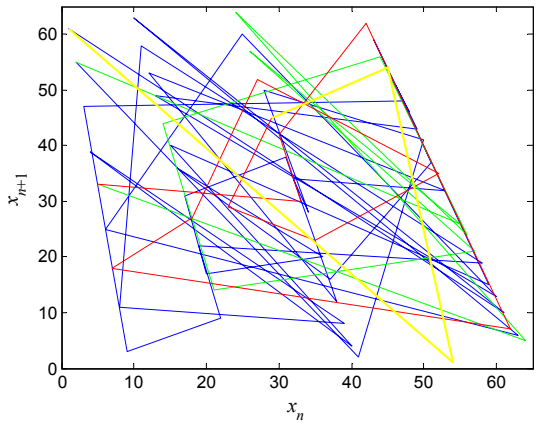

Fig. 3. Chaotic trajectory. N_b=6.

An example of the pseudo-chaotic trajectory is shown in Fig. 3. Parameter d_1 = 0.14, the number of bits is N_b = 6. The order of the concatenated subsequences is blue, green, red and yellow. Every subsequence has contributed by its one period.

4. Computer Experiment

A comparison of an experimental autocovariance $C(m)$ and the ideal autocovariance $C_o(m)$ is shown in Fig. 4. The difference between the experimental $C(m)$ and the optimal $C_o(m)$ is very small for $m \leq 4$. This is due to the fact that quantization errors of the integer-number map had not sufficient effect yet. Behavior of the estimate of the autocovariance $C(m)$ is similar to the behavior of the estimate of the autocovariance for the i.i.d. binary sequence for $m > 4$.

An effect of the tuning of the map on the behavior of RMS and MAE is shown in Fig. 5 for N_b =10. Values of RMS and MAE are irregular with respect to the parameter d_1 provided the step of the parameter d_1 is not too small.

Another simulation has been organized as follows: the 18 maps have been created using different values of d_1. The values of d_1 were closed to 0.15-5g, where

$g = 3.10^{-3}\left(\sqrt{10}\right)^{8-N_b}$. The maps generated the concatenated sequences x. Values of z=30RMS+100MAE were calculated. After that, two sequences with small z were selected.

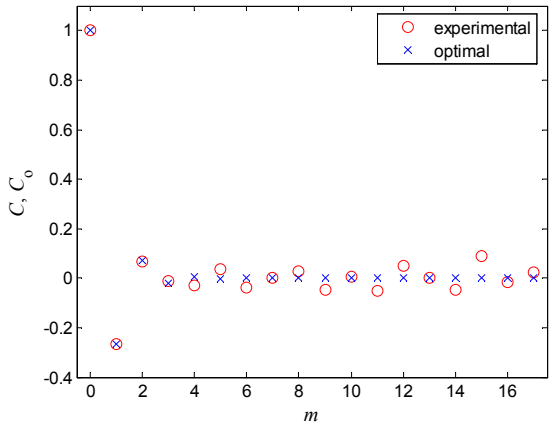

Fig. 4. Comparison of autocovariance $C(m)$ and autocovariance $C_o(m)$. N_b=10.

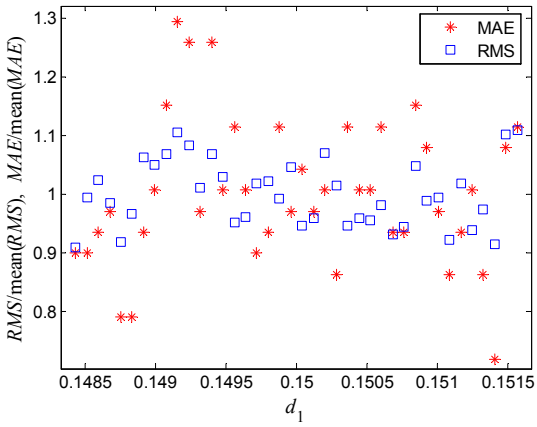

Fig. 5. Influence of the tuning onto behavior of RMS and MAE. N_b =10.

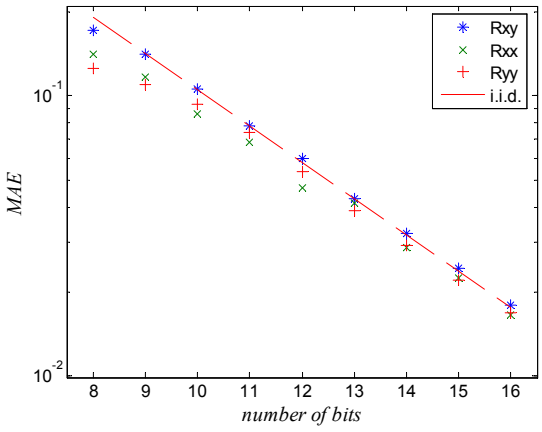

Fig. 6. Maximum absolute error of the correlation versus number of bits N_b.

Then, next 18 maps were created using different d_1. The values of d_1 were closed to 0.15+5g. The maps generated the concatenated sequences y. After that, three sequences with small z were selected. All cross-correlation sequences were calculated using the selected sequences x and y. Finally, the pair of x a y was selected to achieve the minimum value of MAEc.

The quantities MAE and MAEc are drawn in Fig. 6. Both quantities decline for the increasing number of bits N_b. Here, the red dashed line represents MACc of two periodised equiprobable i.i.d. binary sequences. The quantities RMS and RMSc are depicted in Fig. 7. The blue dashed line represents root mean square of the equiprobable i.i.d. binary sequence. The values of all correlation parameters of the concatenated sequences are closed to the corresponding parameters of the equiprobable i.i.d. binary sequences.

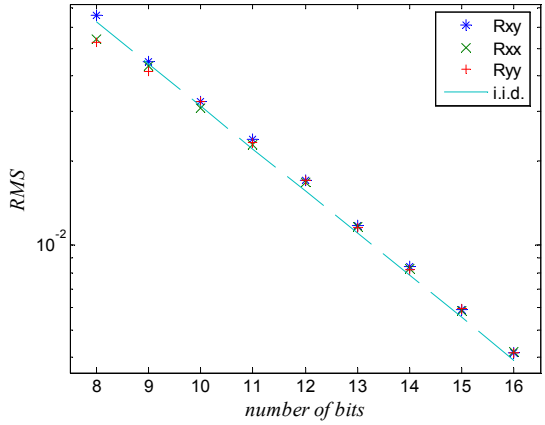

Fig. 7. Root mean square error of the correlation versus number of bits N_b.

Crosscovariance of two different pseudo-chaotic binary sequences is small, even if the difference in their tuning parameters is diminutive. It enables designing numerous sets of the maps.

5. Conclusion

An asymmetrical integer-number map has been reported. The aim was to achieve binary spreading sequence. The tools were tuning the map, quantization of the map, classification and identification of the map, concatenation of the subsequences, quantization of the sequences and suboptimization of the concatenated sequences.

The proposed tuning of the integer-number map is achieved by means of tuning the piece-wise continuous map. Tuning has been used for suboptimizing the integer-number map. The length of the concatenated sequence period is equal to 2^{N_b}. This is advantageous because of constant value of the threshold H and of the perfect balance of the derived binary sequence. Quantization of the se-

quence to achieve the binary sequence can be carried out easily using the most significant bit of every x_n.

The proposed binary sequences have good correlation properties and they are suitable as spreading sequences for the asynchronous DS/CDMA systems. In addition, the number of different sequences is sizable.

Acknowledgements

This research has been supported by the research grant of the Grant Agency of the Czech Republic No. 102/04/0557, by the research grant of the Grant Agency of the Czech Republic No. 102/04/0469 and by the research project Advanced Electronic Communication Systems and Technologies MSM 0021630513.

References

[1] CHUA, L. O. The genesis of Chua's circuit. *Arch. Elektron Ubertragung*, 1992, vol. 46, no. 3, p. 250 - 257.

[2] KENNEDY, M. P. et al. *Chaotic Electronics in Telecommunications*. Boca Raton : CRC Press, 2002, p. 254 - 278.

[3] MASUDA, N., AIHARA, K. Dynamical characteristics of discretized chaotic permutations. *Int. J. Bifurcation and Chaos*, 2002, vol. 12, no 10, p. 2087-2104.

[4] MASUDA, N., AIHARA, K. Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits and Systems – I*, 2002, vol. 49, no. 1, p. 28-40.

[5] KOHDA, T. Information sources using chaotic dynamics. *Proceedings of the IEEE*, 2002, vol. 90, no. 5, p. 641-661.

[6] KOHDA, T., TSUNEDA, A. Statistics of chaotic binary sequences. *IEEE Trans. on Information Theory*, 1997, vol. 43, no. 1, p. 104-111.

[7] ROVATTI, R. et al. Enhanced rake receivers for chaos-based DS-CDMA. *IEEE Transactions on Circuits and Systems - I*, 2001, vol. 48, no. 7, p. 818-829.

[8] AGNELLI, F. et al. A first experimental verification of optimal MAI reduction in chaos-based DS-CDMA systems. In *Proc. ISCAS 2001*, 3, p. 137-140.

[9] TSUNEDA, A. Design of binary sequences with tunable exponential autocorrelations and run statistics based on one-dimensional chaotic maps. *IEEE Transactions on Circuits and Systems - I*, 2005, vol. 52, no. 2, p. 454-462.

[10] YOSHIOKA D., TSUNEDA, A., INOUE, T. Maximal-period sequences with negative auto-correlations and their application to asynchronous DS-CDMA systems. *IEICE Trans. on Fundamentals*, 2003, vol. E87-A, no. 6, p. 1405-1413.

[11] YOSHIOKA D., TSUNEDA, A., INOUE, T. An algorithm for the generation of maximal-period sequences based on one-dimensional chaos map with finite bits. *IEICE Trans. on Fundamentals*, 2004, vol. E87-A, no. 6, p. 1371-1376.

[12] SEBESTA, V. Integer - number maps. In *Radioelektronika 2005, Conference proceedings*. Brno (Czech Republic), 2005, p. 73 – 76.

About Author

Vladimír ŠEBESTA was born in Předín, Czech Republic. He received the M.Sc. degree in electrical engineering from the Czech Technical University, Prague, in 1961 and the Ph.D. degree from the Brno University of Technology in 1974. His research interests include the general areas of statistical signal processing and digital communications. Currently, he is a Professor with the Brno University of Technology, Czech Republic. Prof. Šebesta is a Member of the IEEE.