2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

Chaotic Signal Generation using Orthogonal Functions for Spread Spectrum Communications

Yoshihiro Chatani†, Kohei Okamoto†, Hiroshi Kobayashi† and Hiroyuki Kamata‡

†Graduate School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki 214-8571 Japan
‡School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki 214-8571, Japan,
Email: kamata@isc.meiji.ac.jp

Abstract—In this study, a chaotic signal generator using orthogonal function is proposed, and the property of the generated signal is evaluated based on the viewpoint of suitability into the spread spectrum(SS) communications. An advantageous point that the chaotic signal is adopted to the SS communications is to be able to use various combinations of parameters. In this research, Legendre function is tried to use as the orthogonal function, and compared with the conventional method that Chebyshev function is used.

1. Introduction

The researches that apply the chaotic signal to the spread spectrum communications have been proposed[1, 2]. The advantageous points are as follows;
(a) The spectrum of chaotic signal is widely spread.
(b) The chaotic signals have low cross-correlation property.
(c) Various parameters can be used to generate the chaotic signal compared with M sequence and Gold sequence[3].
However, the characteristic of the signals that the spread spectrum communications request is not only the low correlation-property but also the orthogonality of the signals, so a lot of bit-error in the communications cannot be avoided even if the chaotic signal shows the hyper-chaotic property[4].
Besides, as a method that the orthogonality of the chaotic signal is considered, the research that uses the Chebyshev function[5] to Baker transformation[6] has been proposed[7]. When the system is applied to the SS communications, the correlation property of the signal is improved further. However, when the guarantee of the boundness required to the chaotic map is considered, the number of combinations of parameters, which can be set to the system based on the Chebyshev function, decreases extremely, therefore, one of the advantageous point of the chaotic signals mentioned above is lost. Furthermore, in the case that the finite bit-length arithmetic is used to generate the chaotic signal, the signal often converges to an orbit or a fixed-point even if the Lyapunov exponent becomes a plus value theoretically.
In this study, we propose a method that generates the chaotic signal using Legendre function[5], and compare the property with the system based on the Chebyshev function. The amplitude of signal generated by Legendre function often shows a small numerical value compared with the Chebyshev function, so the Legendre function looks like the one not treated easily. In this research, this problem is solved by devising the function for the numerical expansion used with the Legendre function. Furthermore, it is irrational to prepare the orthogonal polynomial of higher-order as well as the case to use the Chebyshev function. In this study, the differential equation that shows the recurrence relation of the orthogonal function is used, and a practical method which generates the chaotic signal by using the higher-order orthogonal function is shown.

2. Chaotic signal generation using orthogonal functions

Based on the Baker transformation, the method for generating the chaotic signal is shown as follows;
First, the input signal x_n is expanded by

$$y = f(x_n), \qquad (1)$$

and the obtained signal y is folded up by

$$x_{n+1} = P(y). \qquad (2)$$

If the range of value of x_n is equal to the range of x_{n+1}, the boundness of the map is formed. In this study, both of the Chebyshev and Legendre functions are tried to the function $P()$ based on the concept shown in [7].
The Chebyshev function $C_k(x)$ and the Legendre function $L_k(x)$ are shown as

$$C_k(x) = \frac{\sqrt{1-x^2}}{(-1)^k(2k-1)(2k-3)\cdots 1}\frac{d^k}{dx^k}\left(1-x^2\right)^{k-\frac{1}{2}} \qquad (3)$$
$$: k = 0, 1, 2, \cdots$$

and

$$L_k(x) = \frac{1}{2^k k!}\frac{d^k}{dx^k}\left(x^2-1\right)^k : k = 0, 1, 2, \cdots, \qquad (4)$$

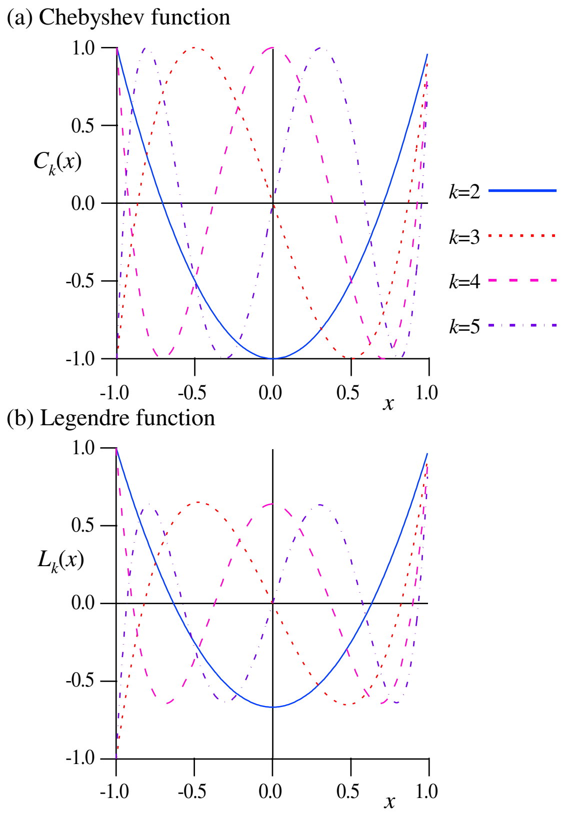

Figure 1: Chebyshev function and Legendre function.

respectively. The forms of these functions are shown in Figure 1.

Besides, preparing the orthogonal polynomials of each order beforehand does not have practical use. In this research, the differential equations, which show the recurrence relation of the orthogonal functions, are used to generate the chaotic signal. The structure of the differential equation is shown in Figure 2, and the differential equation and the coefficients a_k and b_k are as follows:

$$
\begin{aligned}
P_k(x) &= a_k x P_{k-1}(x) - b_k P_{k-2}(x) \\
& \qquad k = 2, 3, \cdots \\
P_1(x) &= x, P_0(x) = 1
\end{aligned} \tag{5}
$$

Chebyshev function:

$$
\left.\begin{aligned} a_k &= 2 \\ b_k &= 1 \end{aligned}\right\} : k = 2, 3, \cdots \tag{6}
$$

Legendre function:

$$
\left.\begin{aligned} a_k &= \tfrac{2k-1}{k} \\ b_k &= \tfrac{k-1}{k} \end{aligned}\right\} : k = 2, 3, \cdots \tag{7}
$$

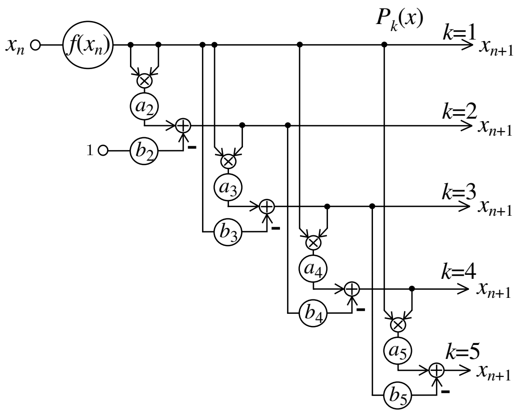

Figure 2: Structure of the chaotic map using the differential equation that shows the recurrence relation of the orthogonal functions.

3. Decision of the Eq. (1)

3.1. The linear equation

As the Figure 1(a) shows, the numerical range is widely spread in $[-1, +1]$ compared with the Legendre function (b), so the Chebyshev function looks like a suitable function to $P(x)$ in the chaotic map. However, the numerical range of the input signal x and the result $C_k(x)$ is both $[-1, +1]$, so the numerical range of $f(x)$ has to be $[-1, +1]$, also. Namely, if the linear equation shown Eq. (8) is adopted to the function $f(x)$,

$$
y = c x_n, \tag{8}
$$

it is necessary to set 1 in the coefficient c to keep the boundness of chaotic map. This property loses merit of using the chaotic signal for the spread spectrum sequence in the viewpoint of the diversity of parameter.

Figure 3 shows the Lyapunov exponent of the chaotic map by Eq. (1) and (2). Eq. (8) is used to Eq. (1). In the figure, the solid-line shows the case that the Chebyshev function is adopted to Eq. (2), and dotted line shows the one that the Legendre function is used. When the Lyapunov exponent is estimated, the derivative of the function $P_k(x)$ shown as follow is used.

$$
\begin{aligned}
P'_k(x) &= a_k \left(P_{k-1}(x) + x P'_{k-1}(x)\right) - b_k P'_{k-2}(x) \\
& \qquad k = 2, 3, \cdots \\
P'_1(x) &= 1, P'_0(x) = 0
\end{aligned} \tag{9}
$$

As the Figure 3 shows, when the Chebyshev function is adopted to the Eq. (2), the area that the boundness is guaranteed is limited to $[-1, +1]$. However, in the case of the Legendre function, the area is expanded following the order k of Legendre function. Namely, if the Legendre function is adopted, the number of parameters that shows the chaotic property is more abundant.

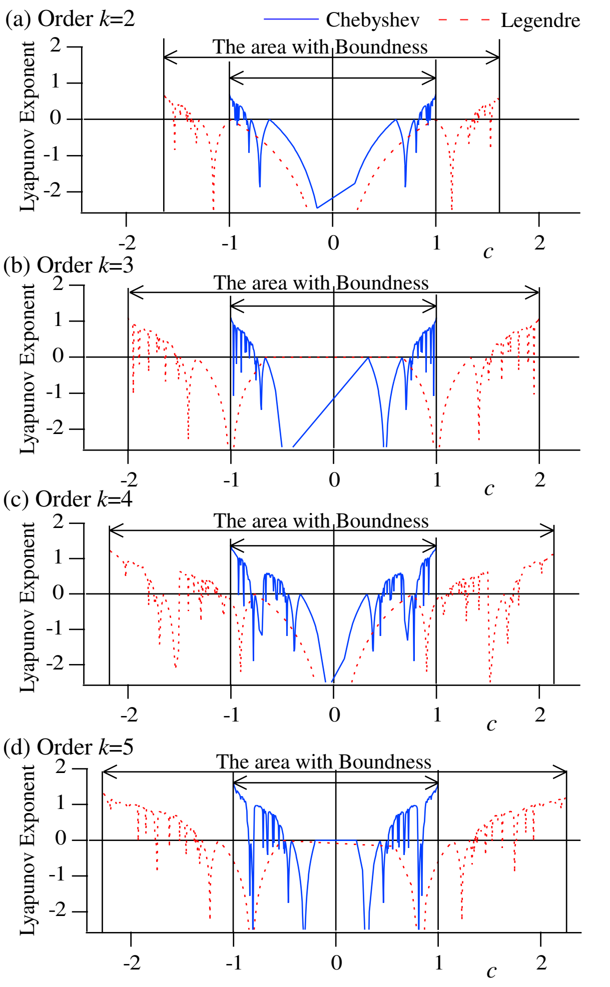

Figure 3: Lyapunov exponent of the chaotic map based on the Eq.(8), (5). Lyapunov exponent is calculated using the data x_n of 10,000[samples].

3.2. The nonlinear equation

When the utilization of the fixed-point arithmetic is assumed, it is needed to consider the overflow in the computation. Then, we try to adopt the nonlinear function shown in Figure 4 to the Eq. (1). The function $O(x)$ in this figure is the overflow function. By using the overflow function, the boundness of the map is always guaranteed without depending on the value of the parameter c. Figure 5 shows the Lyapunov exponent of the chaotic map using the overflow function and the orthogonal function. As the figure shows, the area that shows the boundness is extended compared with the Figure 3. However, the obtained Lyapunov exponents are not the monotonous increase, so it is not possible that the number of effective parameters increases greatly. In the viewpoint, the Lyapunov exponent of the Chebyshev function is larger than the value of Legendre function, so it is more effective as the chaotic map.

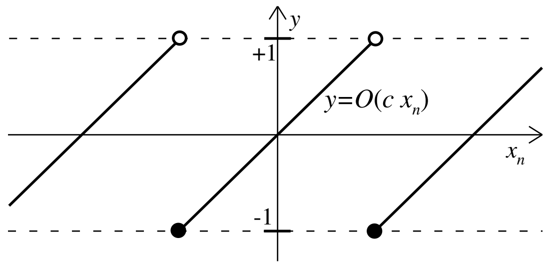

Figure 4: The nonlinear function adopted to the Eq. (1).

(a) Chebyshev function $C_k(x)$ and Overflow function are used

	C_3	C_4	C_5	C_6	C_7	C_8	C_9	Lyapunov Exp.
C_3	413.62	9.5582	24.054	40.824	31.710	57.709	27.110	1.4987
C_4	9.5582	29.257	7.3554	16.283	12.898	14.584	9.6811	1.4987
C_5	24.054	7.3554	479.02	40.516	39.319	79.277	128.12	1.7984
C_6	40.824	16.283	40.516	598.57	102.96	72.352	40.922	1.8292
C_7	31.710	12.898	39.319	102.96	536.09	76.130	40.020	2.0156
C_8	57.709	14.584	79.277	72.352	76.130	528.91	124.42	2.2860
C_9	27.110	9.6811	128.12	40.922	40.020	124.42	492.60	2.2305

(b) Legendre function $L_k(x)$ and Overflow function are used

	L_3	L_4	L_5	L_6	L_7	L_8	L_9	Lyapunov Exp
L_3	94.172	35.109	7.2230	3.5981	1.3007	2.1793	2.4941	1.0002
L_4	35.109	98.135	3.1001	8.4627	18.491	1.2050	1.9672	0.6058
L_5	7.2230	3.1001	53.927	2.9660	0.5276	6.6162	1.4567	1.1024
L_6	3.5981	8.4627	2.9660	58.251	37.402	1.3922	1.7549	0.9791
L_7	1.3007	18.491	0.5276	37.402	96.849	0.9538	4.7588	0.1791
L_8	2.1793	1.2050	6.6162	1.3922	0.9538	31.194	2.1303	1.1684
L_9	2.4941	1.9672	1.4567	1.7549	4.7588	2.1303	61.911	0.8050

Table 1: Correlation properties of the generated chaotic signals. The number of data that is used to the correlation calculation is 1024[samples]. The overflow function is used to Eq. (1), The parameter: $c = 1.98565$, $x_0 = 0.11$. The fixed-point arithmetic of Q14 format is used to the signal generation.

4. Correlation properties of the generated chaotic signals

In this chapter, correlation properties of the generated chaotic signals are investigated. The chaotic signals are generated by using Chebyshev and Legendre functions with overflow function $O(x)$ shown in figure 4.

$$x_{n+1}^k = P_k\left(O(cx_n^k)\right) : k = 3, 4, \cdots, 9 \qquad (10)$$

As the computation accuracy, 16-bit fixed-point arithmetic by Q14 format[4] is adopted. The estimated correlation properties are shown in Table 1. In the table, the maximum values of correlation function $C_{ij}(m)$ are detected and shown.

$$C_{ij}(m) = \sum_{n=0}^{1023} x_n^i x_{n+m}^j : m = 0, 1, \cdots, 1023 \qquad (11)$$
$$i, j = 3, 4, \cdots, 9$$

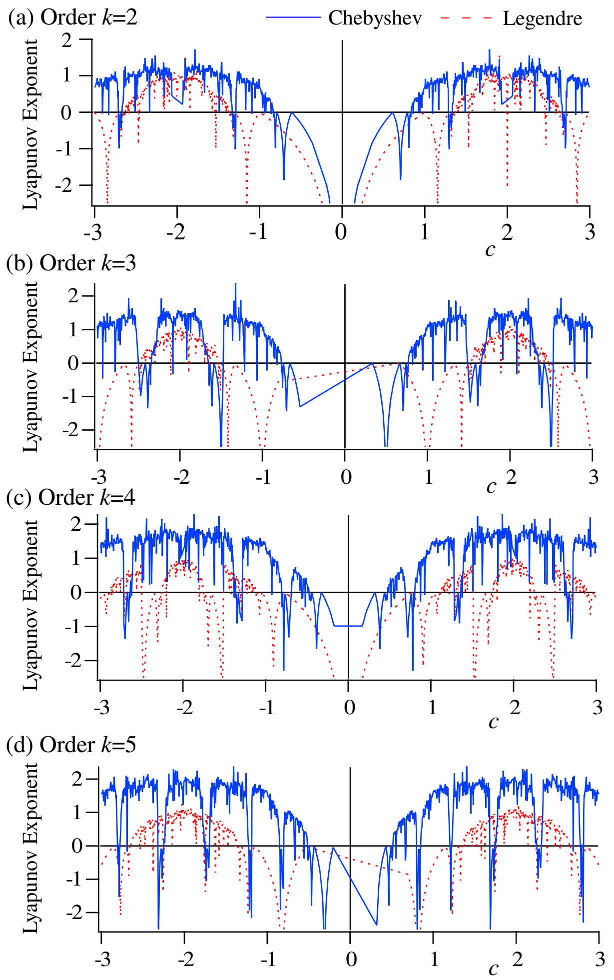

Figure 5: Lyapunov exponent of the chaotic map based on the overflow function shown in figure 4 and Eq. (5). Lyapunov exponent is calculated using the data x_n of 10,000[samples].

As the table shows, the values of auto-correlation of signals generated by using Legendre functions become small because the amplitude of the generated signals are small. However, most of the cross-correlation properties of Legendre functions are relatively better than the case of Chebyshev function. Furthermore, when the Chebyshev function is used, the generated signals x_n often converge on a constant value even if the Lyapunov exponent shows the plus value. Besides, in the case of Legendre function, the convergence to a constant value is few though the amplitude of the generated signal might become small, so we think that Legendre function is suitable to generate the chaotic signal based on the Baker transformation.

5. Conclusions

In this research, the chaotic signal generator by using Legendre function and overflow function has been examined, and compared with the system using Chebyshev function. The system with Chebyshev function has a excellent feature in the point to guarantee the boundness easily. However, the flexibility of the parameter setting is insufficient as long as overflow function is not used to the Eq. (1). Furthermore, the generated signals often converge on a constant value, so we think that this system with Chebyshev function is not necessarily practicable.
Besides, in the case of the system that uses Legendre function, the convergence to a constant value is few though the amplitude of the generated signal might become small. In addition, the correlation property of the generated signal is better than the system by Chebyshev function, so we think that the system using Legendre function is suitable to generate the signals for spread spectrum communications.
As the next problem, we intend to apply the proposed system to the SS sequence, and the property of the proposed method is compared with the conventional system based on M and Gold sequences.

References

[1] H. Dedieu, M. P. Kennedy and M. H. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits", *IEEE Trans. CAS. Part-II*, Vol. 40, No.10, pp.634-642, 1993.

[2] G. Kolumban, B. Vizvari, W. Schwarz and A. Abel, "Differential chaos shift keying: a robust coding for chaotic communication", *Proc. Int. Workshop on Nonlinear Dynamics of Electronic Systems*, pp.87-92, 1996.

[3] K. Tsutsumi, T. Murotani, H. Kamata and T. Endo, "Verification of Randomness on Pseudo Chaotic Signals Generated by Digital System", *IEICE Technical Report*, SST2002-59, pp.51-56, 2000(Japanese).

[4] H. Kamata, Y. Umezawa, M. Dobashi, T. Endo and Y. Ishida, "Private communications with chaos based on the fixed-point computation" *IEICE, Trans. IEICE*, Vol. E83-A, No. 6, 2000.

[5] http://mathworld.wolfram.com/Orthogonal-Polynomials.html

[6] Y. Aizawa and C. Murakami, "Generalization of Baker's transformation-chaos and stochastic processon a Smale's horse-shoe", *Prog. Theor. Phys.*, vol.69, no.5,pp.1416-26, 1983.

[7] K. Umeno, H. L. Lin and S. H. Shih, "Fixed-Point Implementation of Chebyshev Sequence Generators with Applications to DS-CDMA and Giga bit/s Vector Stream Ciphers" *IEICE, Proc. NOLTA 2002*, N1-5-6, 2002.