IEICE Proceeding Series

Study on Auto-Correlation Functions of Low-Density Binary Sequences Generated by Bernoulli Map and Nonlinear Feedback Shift Registers

Akio Tsuneda, Shogo Inada

Vol. 1 pp. 895-898
Publication Date: 2014/03/17
Online ISSN: 2188-5079

2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

Study on Auto-Correlation Functions of Low-Density Binary Sequences Generated by Bernoulli Map and Nonlinear Feedback Shift Registers

Akio Tsuneda and Shogo Inada

Department of Computer Science and Electrical Engineering, Kumamoto University
2–39–1 Kurokami, Chuo-ku, Kumamoto, 860–8555 JAPAN
E-mail: tsuneda@cs.kumamoto-u.ac.jp

Abstract—Auto-correlation functions of *low-density* binary sequences generated by Bernoulli map and nonlinear feedback shift registers are discussed in this paper. First, we theoretically evaluate auto-correlation functions of low-density chaotic binary sequences generated by Bernoulli map based on chaos theory. Next, we numerically evaluate auto-correlation functions of low-density periodic binary sequences generated by nonlinear feedback shift registers (NFSRs).

1. Introduction

Chaotic binary sequences with various correlation properties can be designed by using a class of chaotic maps and binary functions [1]. Chaotic binary sequences can be applied to CDMA communications, cryptosystems, and Monte-Carlo simulations. Basically, in these applications, chaotic binary sequences are designed as balanced sequences, that is, the probability of 1 (or 0) in the sequences is equal to $\frac{1}{2}$.

On the other hand, LDPC (low density parity check) codes [2], which have been attracting attention recently, is specified by a parity-check matrix with mostly 0's and relatively few 1's. One of methods to construct row (or column) vectors of such a parity-check matrix of LDPC codes is to use random numbers. Chaotic sequences can also be used for constructing LDPC codes [3].

In this paper, we first evaluate auto-correlation functions of low-density chaotic binary sequences generated by the Bernoulli map based on chaos theory. Next, we evaluate auto-correlation functions of low-density periodic binary sequences generated by nonlinear feedback shift registers (NFSRs) which can be regarded as finite bit realization of the Bernoulli map [4].

2. Low-Density Chaotic Binary Sequences Generated by Bernoulli Map

Using a one-dimensional nonlinear difference equation defined by

$$x_{n+1} = \tau(x_n),\ x_n \in I = [d, e],\ n = 0, 1, 2, \cdots, \qquad (1)$$

we can generate a *chaotic* real-valued sequence $\{x_n\}_{n=0}^{\infty}$, where $x_n = \tau^n(x)$ ($x_0 = x$ is an initial value). We transform such a real-valued sequence into a binary sequence $\{B(x_n)\}_{n=0}^{\infty}$ by using a binary function $B(x)$ ($\in \{0, 1\}$). The theoretical auto-correlation function of such a binary sequence $\{B(x_n)\}_{n=0}^{\infty}$ is defined by

$$C(\ell; B) = \int_I (B(x) - \langle B\rangle)(B(\tau^\ell(x)) - \langle B\rangle) f^*(x)dx, \qquad (2)$$

under the assumption that $\tau(x)$ has an invariant density function $f^*(x)$, where $\langle B\rangle$ denotes the expectation of the binary sequence $\{B(x_n)\}_{n=0}^{\infty}$ defined by

$$\langle B\rangle = \int_I B(x) f^*(x)dx. \qquad (3)$$

In this paper, we also use the normalized auto-correlation function defined by $R(\ell; B) = C(\ell; B)/C(0; B)$.

Here, we use the Bernoulli map $\tau(x)$ defined by

$$\tau(x) = \begin{cases} 2x & (0 \le x < \frac{1}{2}) \\ 2x - 1 & (\frac{1}{2} \le x \le 1) \end{cases} \qquad (4)$$

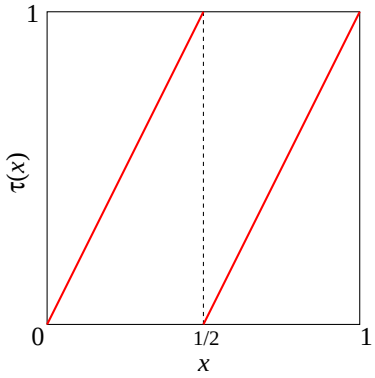


Figure 1: Bernoulli map

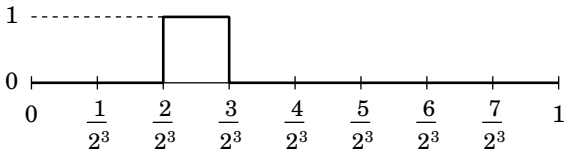


Figure 2: An example of binary functions given by eq.(5) ($m = 3$, $i = 2$)

Table 1: Theoretical normalized auto-correlation functions $R(\ell; B_i^{(3)})$

ℓ	1	2	$3, \cdots$
$B_0^{(3)}$	3/7	1/7	0
$B_1^{(3)}$	−1/7	−1/7	0
$B_2^{(3)}$	−1/7	1/7	0
$B_3^{(3)}$	−1/7	−1/7	0
$B_4^{(3)}$	−1/7	−1/7	0
$B_5^{(3)}$	−1/7	1/7	0
$B_6^{(3)}$	−1/7	−1/7	0
$B_7^{(3)}$	3/7	1/7	0

Table 2: Theoretical normalized auto-correlation functions $R(\ell; B_i^{(4)})$

ℓ	1	2	3	$4, \cdots$
$B_0^{(4)}$	7/15	1/5	1/15	0
$B_1^{(4)}$	−1/15	−1/15	−1/15	0
$B_2^{(4)}$	−1/15	−1/15	1/15	0
$B_3^{(4)}$	−1/15	−1/15	−1/15	0
$B_4^{(4)}$	−1/15	−1/15	1/15	0
$B_5^{(4)}$	−1/15	1/5	−1/15	0
$B_6^{(4)}$	−1/15	−1/15	1/15	0
$B_7^{(4)}$	−1/15	−1/15	−1/15	0
$B_8^{(4)}$	−1/15	−1/15	−1/15	0
$B_9^{(4)}$	−1/15	−1/15	1/15	0
$B_{10}^{(4)}$	−1/15	1/5	−1/15	0
$B_{11}^{(4)}$	−1/15	−1/15	1/15	0
$B_{12}^{(4)}$	−1/15	−1/15	−1/15	0
$B_{13}^{(4)}$	−1/15	−1/15	1/15	0
$B_{14}^{(4)}$	−1/15	−1/15	−1/15	0
$B_{15}^{(4)}$	7/15	1/5	1/15	0

which is one of the simplest piecewise linear chaotic maps with the interval $I = [0, 1]$ and $f^*(x) = 1$. The map is shown in Fig.1. As will be shown later, the Bernoulli map can be approximated by NFSRs with finite bits.

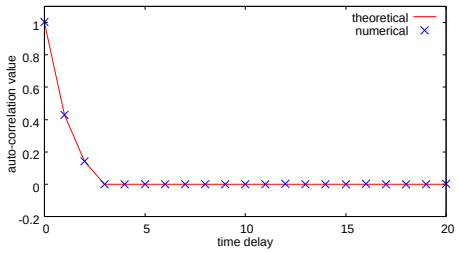
Furthermore, we use binary functions defined by

$$B_i^{(m)}(x) = \Theta_{\frac{i}{2^m}}(x) - \Theta_{\frac{i+1}{2^m}}(x) \quad (i = 0, 1, \cdots, 2^m - 1), \tag{5}$$

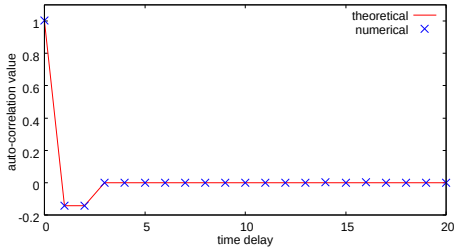
where m is a positive integer and $\Theta_t(x)$ is a threshold function defined by

$$\Theta_t(x) = \begin{cases} 1 & (x \geq t) \\ 0 & (x < t). \end{cases} \tag{6}$$

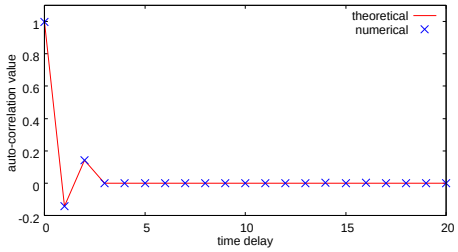
An example of such binary functions is shown in Fig.2, where $m = 3$ and $i = 2$ (*i.e.*, $B_2^{(3)}(x)$). Since the invariant density function of the Bernoulli map is $f^*(x) = 1$, the expectation (probability of 1) of the binary sequences



(a) $i = 0$



(b) $i = 1$



(c) $i = 2$

Figure 3: Numerical results of normalized auto-correlation functions $R(\ell; B_i^{(3)})$

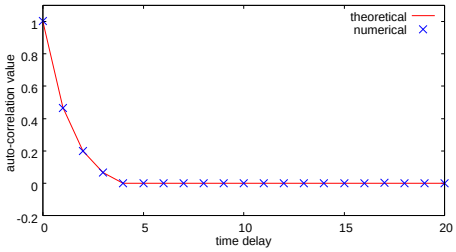
$\{B_i^{(m)}(x_n)\}_{n=0}^{\infty}$ is given by $\langle B_i^{(m)} \rangle = 2^{-m}$, which implies the sequences are *low-density* binary sequences for $m \geq 2$.

We theoretically evaluate the low-density auto-correlation functions of the binary sequences $\{B_i^{(m)}(x_n)\}_{n=0}^{\infty}$ using Perron-Frobenius operator [5]. Consequently, the normalized auto-correlation functions are given by

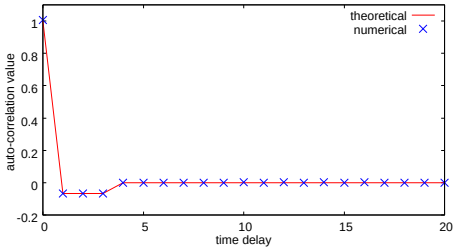
$$R(\ell; B_i^{(m)}) = \begin{cases} \dfrac{2^{m-\ell} - 1}{2^m - 1} & (\lfloor \frac{i}{2^\ell} \rfloor = i \bmod 2^{m-\ell}) \\ -\dfrac{1}{2^m - 1} & (\lfloor \frac{i}{2^\ell} \rfloor \neq i \bmod 2^{m-\ell}) \\ 0 & (\ell \geq m), \end{cases} \tag{7}$$

where $\lfloor x \rfloor$ denotes the largest integer not exceeding x. Tables 1 and 2 show the results for the cases $m = 3$ and $m = 4$, respectively. From these tables, we find that there are binary sequences with positive and negative auto-correlations but there are no uncorrelated sequences.

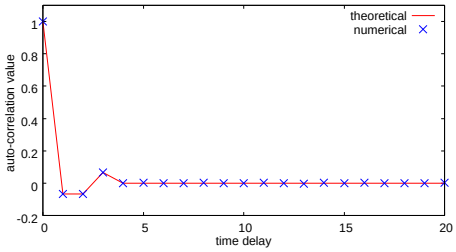
We also numerically evaluate the auto-correlation functions of the binary sequences $\{B_i^{(m)}(x_n)\}_{n=0}^{N-1}$ using a computer with 64-bit floating operation, where we set $N = 1,000,000$. Figures 3 and 4 show the numerical results with the theoretical functions. The numerical results are in good agreement with the theoretical ones.



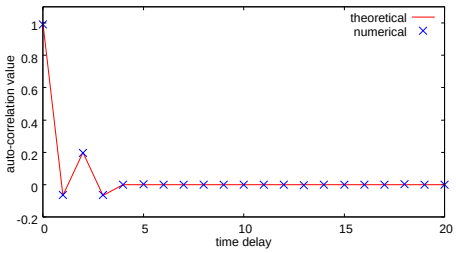
(a) $i = 0$



(b) $i = 1$



(c) $i = 2$



(d) $i = 5$

Figure 4: Numerical results of normalized auto-correlation functions $R(\ell; B_i^{(4)})$

3. Low-Density Periodic Binary Sequences Generated by NFSRs

Figure 5 shows a k-stage NFSR whose feedback circuit is nonlinear (a combinational logic circuit). Maximal-period binary sequences of period 2^k generated by k-stage NFSRs are called *de Bruijn sequences* [6].

Let us transform a state of the register at time n, denoted by $\{a_{k-1}(n), a_{k-2}(n), \cdots, a_0(n)\}$, into a decimal integer $\hat{x}_n \in [0, 2^k - 1]$ as

$$\hat{x}_n = a_0(n) \cdot 2^{k-1} + a_1(n) \cdot 2^{k-2} + \cdots + a_{k-1}(n) \cdot 2^0. \quad (8)$$

Plotting $(\hat{x}_n, \hat{x}_{n+1})$ for an NFSR, we can obtain a one-dimensional (1-D) map (so called, *return map*). An example of such maps is shown in Fig.6, where $k = 4$. It is

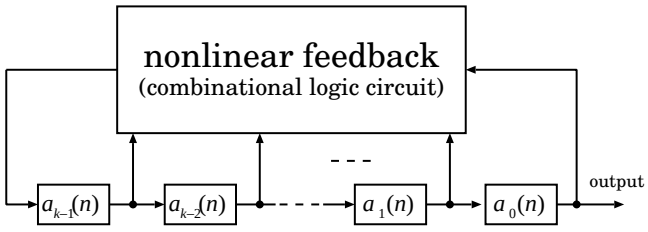


Figure 5: k-stage nonlinear feedback shift register

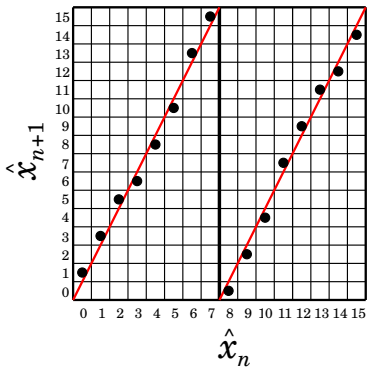


Figure 6: An example of 1-D return map of NFSRs ($k = 4$)

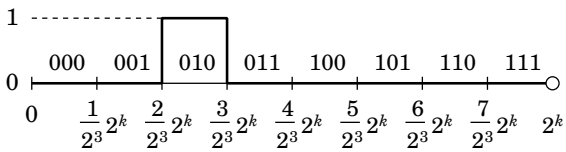


Figure 7: An example of binary functions given by eq.(9) ($m = 3$, $i = 2$)

easy to understand that the shapes of such 1-D return maps are similar to the Bernoulli map denoted by solid lines, which implies that the NFSRs approximate the Bernoulli map with finite bits [4].

Noting that an integer sequence $\{\hat{x}_n\}_{n=0}^{2^k-1}$ generated by a k-stage NFSR corresponds to a real-valued sequence $\{x_n\}_{n=0}^{\infty}$ generated by the Bernoulli map, we define binary functions for such a maximal-period integer sequence $\{\hat{x}_n\}_{n=0}^{2^k-1}$ by

$$\hat{B}_i^{(m)}(x) = \Theta_{\frac{i}{2^m}2^k}(x) - \Theta_{\frac{i+1}{2^m}2^k}(x) \quad (i = 0, 1, \cdots, 2^m - 1), \quad (9)$$

where $m \leq k$. An example of such binary functions is shown in Fig.7, where $m = 3$ and $i = 2$ (*i.e.*, $\hat{B}_2^{(3)}(x)$). Note that $\hat{B}_i^{(m)}(x)$ can be realized by a combinational logic circuit with m inputs, where m inputs are the most m significant bits of the NFSR, that is, $\{a_0(n), a_1(n), \cdots, a_{m-1}(n)\}$. For example, the binary function $\hat{B}_2^{(3)}(x)$ in Fig.7 can also be written as

$$\hat{B}_2^{(3)}(x) = \begin{cases} 1 & \text{if } a_0(n)a_1(n)a_2(n) = 010 \\ 0 & \text{otherwise.} \end{cases} \quad (10)$$

Since each integer in $\{0, 1, \cdots, 2^k - 1\}$ appears once in a period of a maximal-period integer sequence $\{\hat{x}_n\}_{n=0}^{2^k-1}$

Table 3: Normalized auto-correlation values $\hat{R}(\ell;\hat{B}_i^{(3)})$ for some de Bruijn sequences of period 64 generated by 6-stage NFSRs.

i	ℓ	DB1	DB2	DB3	chaos
0 (000)	1	3/7	3/7	3/7	3/7
	2	1/7	1/7	1/7	1/7
	3	0	0	0	0
	4	0	0	−1/7	0
1 (001)	1	−1/7	−1/7	−1/7	−1/7
	2	−1/7	−1/7	−1/7	−1/7
	3	0	0	0	0
	4	−1/7	−1/7	1/7	0
2 (010)	1	−1/7	−1/7	−1/7	−1/7
	2	1/7	1/7	1/7	1/7
	3	0	0	0	0
	4	−1/7	−1/7	0	0
3 (011)	1	−1/7	−1/7	−1/7	−1/7
	2	−1/7	−1/7	−1/7	−1/7
	3	0	0	0	0
	4	1/7	−1/7	1/7	0
4 (100)	1	−1/7	−1/7	−1/7	−1/7
	2	−1/7	−1/7	−1/7	−1/7
	3	0	0	0	0
	4	−1/7	−1/7	1/7	0
5 (101)	1	−1/7	−1/7	−1/7	−1/7
	2	1/7	1/7	1/7	1/7
	3	0	0	0	0
	4	1/7	1/7	0	0
6 (110)	1	−1/7	−1/7	−1/7	−1/7
	2	−1/7	−1/7	−1/7	−1/7
	3	0	0	0	0
	4	1/7	1/7	−1/7	0
7 (111)	1	3/7	3/7	3/7	3/7
	2	1/7	1/7	1/7	1/7
	3	0	0	0	0
	4	−1/7	−1/7	−1/7	0

of period 2^k, the probability of 1 in a binary sequence $\{\hat{B}_i^{(m)}(\hat{x}_n)\}_{n=0}^{2^k-1}$ (or the average of the sequence) is equal to 2^{-m}, which also corresponds to the binary sequence $\{B_i^{(m)}(x_n)\}_{n=0}^{\infty}$ generated by the Bernoulli map. Note that the number of 1's in the sequence $\{\hat{B}_i^{(m)}(\hat{x}_n)\}_{n=0}^{2^k-1}$ is exactly equal to 2^{k-m}.

Now we define the periodic auto-correlation function of a binary sequence $\{\hat{B}_i^{(m)}(\hat{x}_n)\}_{n=0}^{N-1}$ of period $N = 2^k$ whose average is 2^{-m} by

$$\hat{C}(\ell;\hat{B}_i^{(m)}) = \frac{1}{N}\sum_{n=0}^{N-1}(\hat{B}_i^{(m)}(\hat{x}_n)-2^{-m})(\hat{B}_i^{(m)}(\hat{x}_{(n+\ell) \bmod N}-2^{-m}). \tag{11}$$

Also, the normalized periodic auto-correlation function is defined by $\hat{R}(\ell;\hat{B}_i^{(m)}) = \hat{C}(\ell;\hat{B}_i^{(m)})/\hat{C}(0;\hat{B}_i^{(m)})$. We numerically evaluate the periodic auto-correlation functions of the low-density binary sequences $\{\hat{B}_i^{(m)}(\hat{x}_n)\}_{n=0}^{2^k-1}$ generated by k-stage NFSRs, where $k = 6$ and $m = 3$. Table 3 shows the normalized auto-correlation values $\hat{R}(\ell;\hat{B}_i^{(3)})$ ($\ell = 1 \sim 4$) for three different de Bruijn sequences (denoted by "DB1", DB2", and "DB3") of period 64. In the table, the column denoted by "chaos" shows the theoretical values given in Table 1. There are some different auto-correlation values at $\ell = 4$ for the three de Bruijn sequences. However, the auto-correlation values for $\ell \le 3$ are equal to each other and they are exactly equal to the theoretical values.

4. Conclusion

We theoretically and numerically evaluate auto-correlation functions of low-density chaotic binary sequences generated by Bernoulli map. We also numerically evaluate auto-correlation functions of low-density periodic binary sequences generated by NFSRs. It is remarkable that the auto-correlation values of low-density periodic binary sequences generated by NFSRs are completely equal to the theoretical ones for small time delays. The application of such periodic low-density binary sequences to LDPC codes is a future topic.

Acknowledgments

This work was partly supported by Grant-in-Aid for Scientific Research (C) (No.23560460) from Japan Society for the Promotion of Science.

References

[1] A. Tsuneda, "Design of Binary Sequences With Tunable Exponential Autocorrelations and Run Statistics Based on One-Dimensional Chaotic Maps," *IEEE Trans. Circuits Syst. I*, vol.52, no.2, pp.454–462, 2005.

[2] R. G. Gallager, "Low-Density Parity-Check Codes," *IRA Trans. Inf. Theory*, vol.8, no.1, pp.21–28, 1962.

[3] S. Kozic, M. Hasler, "Low-Density Codes Based on Chaotic Systems for Simple Encoding," *IEEE Trans. Circuits Syst. I*, vol.56, no.2, pp.405–415, 2009.

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

[5] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise*, Springer-Verlag, 1994.

[6] S. W. Golomb, *Shift Register Sequences*, revised ed., Aegean Park Press,1982.