Fast Generation of Binary Random Sequences by Use of Random Sampling Method

Hiroshi Harada and Hiroshi Kashiwagi**

* *Faculty of Engineering, Kumamoto University, 2-39-1 Kurokami,*
Kumamoto, 860, Japan, Phone: +81-096-344-2111 ext. 3747

Abstract

A new method for generation of binary random sequences, called random sampling method, has been proposed by the authors. However, the random sampling method has the defect that binary random sequence can not be rapidly generated. In this paper, two methods based on the random sampling method are proposed for fast generation of binary random sequences. The optimum conditions for obtaining ideal binary random sequences are derived.

1. Introduction

Binary random sequences are widely used as the modulation codes for continuous wave radar or spread-spectrum communication system. A new method, called random sampling method, has been proposed by the authors for generation of binary random sequences having good randomness property [1],[2]. In this method, the binary random sequences are generated by use of an arbitrary binary sequence and uniform random numbers. The optimum conditions for obtaining ideal binary random sequences having good random properties were introduced [3]. However, the random sampling method has the defect that since only one element of a binary sequence is obtained for one uniform random number, binary random sequences can not be rapidly generated.

In this paper, two methods based on the random sampling method are proposed for fast generation of binary random sequence. The expected values of autocorrelation function of the binary random sequence generated by the proposed methods are derived theoretically. From these theoretical values, optimum conditions are derived for generating binary random sequences having good random properties.

2. Random sampling method

Let us briefly review the random sampling method proposed in reference [1]. Let $\{a_i\}$ denote an arbitrary periodical binary sequence and N be the period of $\{a_i\}$

$$\{a_i\} = a_0, a_1, \cdots, a_{N-1} \qquad (a_i = 0 \text{ or } 1)$$

Then, successive k-tuples $\boldsymbol{a}_{ki}$ $(i = 0, 1, \cdots)$ are generated as

$$\boldsymbol{a}_{ki} = (a_{ki}, a_{ki+1}, \cdots, a_{ki+k-1}) \tag{1}$$

Using a random number X_i $(i = 0, 1, \cdots)$, which is distributed uniformly between 0 and 1, $([k \cdot X_i] + 1)$-th bit of $\boldsymbol{a}_{ki}$ is chosen and become i-th element of a binary random sequence. Here, $[k \cdot X_i]$ denotes the maximum integer less than $k \cdot X_i$. In the random sampling method, binary random sequences are generated by this procedure.

Let $\{r_i\}$ be the binary random sequence generated by this method, then $\{r_i\}$ can be expressed as

$$\{r_i\} = a_{[k \cdot X_0]}, a_{k+[k \cdot X_1]}, \cdots, a_{ki+[k \cdot X_i]}, \cdots$$

Autocorrelation function (ACF) of the sequence $\{r_i\}$ is defined [4] as,

$$\phi_{rr}(\tau) = \frac{1}{L} \sum_{i=0}^{L-1} (-1)^{r_i} \cdot (-1)^{r_{i+\tau}} \tag{2}$$

Here, L is a sample size which, in this paper, is equal to 128. The expected values of the ACF (EACF) of the sequence $\{r_i\}$ is given as eqn. (3) [1],[2].

$$E[\phi_{rr}(\tau)] = \frac{1}{Lk^2} \sum_{i=0}^{L-1} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} (-1)^{a_{ki+j}} \cdot (-1)^{a_{k(i+\tau)+l}} \tag{3}$$

When the tuple length k is equal to the period N of the original binary sequence $\{a_i\}$,

$$a_{Ni+j} = a_j, \quad a_{N(i+\tau)+l} = a_l$$

Substituting these equations into eqn. (3), the EACF of the binary random sequence $\{r_i\}$ is given by the next equation.

$$\begin{aligned} E[\phi_{rr}(\tau)] &= \frac{1}{LN^2} \sum_{i=0}^{L-1} \sum_{j=0}^{N-1} \sum_{l=0}^{N-1} (-1)^{a_j} \cdot (-1)^{a_l} \\ &= \frac{1}{N^2} \{ \sum_{j=0}^{N-1} (-1)^{a_j} \}^2 \\ &= (\frac{c_1 - c_0}{N})^2 \end{aligned} \tag{4}$$

Here, c_1 is the number of 1's in a period of the original binary sequence and c_0 is that of 0's. If the original binary sequence $\{a_i\}$ includes 1's and 0's equally in a period, substitution of $c_1 = c_0$ into eqn. (4) yields

$$E[\phi_{rr}(\tau)] = 0$$

In this case, the generated binary random sequence shows the best randomness.

3. Fast generatinon of binary random sequences

In the previous section, it is shown that binary random sequences having good random properties can be obtained by use of the random sampling method. The defect of the random sampling method is that the binary random sequences can not be rapidly generated. This is because of the fact that only one element of a binary random sequence is obtained from one uniform random number. In this section, two methods based on the random sampling method are proposed for fast generation of binary random sequences.

In this paper, it is supposed that the following two condistions are satisfied.

i. Uniform random numbers $\{X_i\}$ distribute uniformly in two-dimensional space.

ii. Binary sequence $\{a_i\}$ includes 1's and 0's equally in a period.

If these conditions are satisfied, binary random sequences having random properties can be always obtained by the random sampling method.

3.1 Method A

The first method, called method A, is to choose a k-tuple of a binary sequence $\{a_i\}$ randomly. The k-tuples of $\{a_i\}$ are defined by eqn. (1). By use of a uniform random number $X_i (0 \leq X_i < 1)$, $([N \cdot X_i] + 1)$-th k-tuple is chosen and all elements of the k-tuple become the elements of binary random sequence. Then, k bits of a binary random sequence can be generated by a uniform random number X_i. Let $\{q_i\}$ be a binary random sequence generated by method A, $\{q_i\}$ can be expressed as

$$\{q_i\} = \underbrace{a_{[N\cdot X_0]}, \cdots a_{[N\cdot X_0]+k-1}}_{\overset{\shortparallel}{\boldsymbol{a}_{[N\cdot X_0]}}}, \underbrace{a_{[N\cdot X_1]}, \cdots a_{[N\cdot X_1]+k-1}}_{\overset{\shortparallel}{\boldsymbol{a}_{[N\cdot X_1]}}} \cdot \cdots$$

(i) In case of the delay $\tau \geq k$, the i-th element of the binary random sequence and the $(i + \tau)$-th one are sampled from different k-tuples. The delay τ can be expressed as

$$\tau = \lambda \cdot k + \mu$$

$$\lambda = \tau / k, \quad \mu = (\text{mod } \tau, k)$$

Then, the expected value of $(-1)^{q_{i+\tau}}$ is given as

$$E[(-1)^{q_{i+\tau}}] = \frac{1}{N} \sum_{\sigma=0}^{N-1} (-1)^{a_{\sigma+m+\mu}} = 0 \qquad (9)$$

Substituting eqns. (8) and (9) into eqn. (6), EACF of $\{q_i\}$ is given by the next equation.

$$E[\phi_{qq}(\tau)] = \frac{1}{L \cdot N^2} \sum_{j=0}^{N-1} \sum_{\sigma=0}^{N-1} (-1)^{a_{j+m}} \cdot (-1)^{a_{\sigma+m+\mu}}$$
$$= 0 \qquad (10)$$

(ii) In case of the delay $\tau \leq k - 1$, if τ is smaller than $k - m$, the i-th and the $(i + \tau)$-th element of $\{p_i\}$ are sampled from the same k-tuple. Then, the expected value of $(-1)^{q_i} \cdot (-1)^{q_{i+\tau}}$ is gien as

$$E[(-1)^{q_i} \cdot (-1)^{q_{i+\tau}}]$$
$$= \frac{\tau}{N^2 \cdot k} \sum_{m=k-\tau}^{k-1} \sum_{j=0}^{N-1} \sum_{\sigma=0}^{N-1} (-1)^{a_{j+m}} \cdot (-1)^{a_{\sigma+m+\tau}}$$
$$+ \frac{k-\tau}{N \cdot k} \sum_{m=0}^{k-\tau-1} \sum_{j=0}^{N-1} (-1)^{a_{j+m}} \cdot (-1)^{a_{j+m+\tau}} \qquad (11)$$

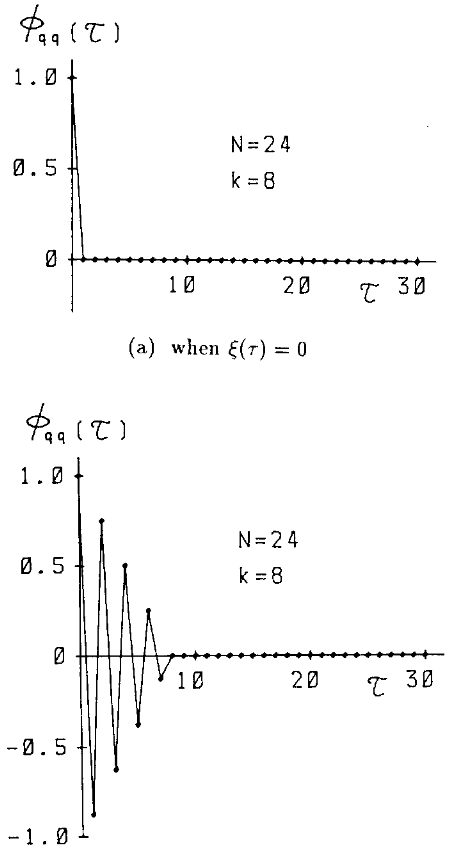
The first term of the right-hand side of eqn. (11) becomes 0 if the conditions i. and ii. are satisfied. However, the value of the second term of eqn. (11) depends on the arrangement of 1's and 0's included in a period of $\{a_i\}$, and it is not always equal to 0. Let $\xi(\tau)$ $(1 \leq \tau \leq k - 1)$ be defined as

$$\xi(\tau) \equiv \sum_{m=0}^{k-\tau-1} \sum_{j=0}^{N-1} (-1)^{a_{j+m}} \cdot (-1)^{a_{j+m+\tau}} \qquad (12)$$

Substituting eqns. (11) and (12) into eqn. (6), EACF of $\{q_i\}$ is given by the next equation.

$$E[\phi_{qq}(\tau)] = \frac{k-\tau}{N \cdot k} \xi(\tau) \qquad (13)$$

Examples of EACF of $\{q_i\}$ are shown in Fig.1.



(a) when $\xi(\tau) = 0$

(b) when $\xi(\tau) \neq 0$

Fig.1 EACF of binary sequence $\{q_i\}$

Here, the tuple length k is equal to 8 and the period N of the original binary sequence $\{a_i\}$ is equal to 24. In case of Fig.1 (a), the original binary sequence $\{a_i\}$ is chosen to satisfy the next equation.

$$\xi(\tau) = 0 \quad (0 \leq \tau \leq k-1) \tag{14}$$

Then, from eqns. (10) and (13), EACF of $\{q_i\}$ is equal to the δ-function. On the other hand, EACF of $\{q_i\}$ shown in Fig.1 (b) is not equal to 0·when the delay τ is smaller than the tuple length k, since the original binary sequence $\{a_i\}$ does not satisfy eqn. (14).

From these results, the original binary sequence $\{a_i\}$ must satisfy eqn. (14),in order to generate binary random sequences having good randomness propertiesby method A.

3.2 Method B

The second method, called method B, is to use a multi-valued sequence instead of a binary sequence. Let $\{b_i\}$ be a P-valued sequence.

$$\{b_i\} = b_0, b_1, \cdots, b_{N-1} \qquad (0 \leq b_i \leq P-1)$$

In this paper, it is assumed that the multi-valued sequence $\{b_i\}$ includes every value i $(0 \leq i \leq P-1)$ equally in a period N. So, the period N becomes

$$N = j \cdot P \quad (j : \text{positive integer})$$

The i-th element of the multi-valued sequence $\{b_i\}$ can be expressed by the next equation.

$$b_i = \sum_{j=0}^{k-1} b_{i,j} \cdot 2^j \qquad (b_{i,j} = 0 \ \text{ or } \ 1) \tag{15}$$

In method B, one uniform random number $X_i (0 \leq X_i < 1)$ is generated and $([N \cdot X_i] + 1)$-th element of $\{b_i\}$ is chosen. Then, the sampled element of the multi-valued sequence is transformed into k bits of a binary random sequence by use of eqn. (15). Let $\{p_i\}$ be a binary random sequence generated by method B, $\{p_i\}$ can be expressed as

$$\{p_i\} = \underbrace{b_{[N\cdot X_0],0}, \cdots b_{[N\cdot X_0],k-1}}_{\overset{\shortparallel}{b_{[N\cdot X_0]}}}, \underbrace{b_{[N\cdot X_1],0}, \cdots b_{[N\cdot X_1],k-1}}_{\overset{\shortparallel}{b_{[N\cdot X_1]}}} \cdot \cdots$$

EACF of $\{p_i\}$ is also given by equation (16)

$$E[\phi_{pp}(\tau)] = \frac{1}{L} \sum_{i=0}^{L-1} E[(-1)^{p_i} \cdot (-1)^{p_{i+\tau}}] \tag{16}$$

and can be calculated theoretically as follows.

(i) In case of the delay $\tau \geq k$, p_i and $p_{i+\tau}$ are obtained from different elements of the multi-valued sequence $\{b_i\}$. Since i can be expressed by eqn. (7), the i-th element of the binary random sequence $\{p_i\}$ becomes

$$p_i = b_{[N\cdot X_l],m}$$

Then, the expected value of $(-1)^{p_i}$ is given by eqn. (17).

$$E[(-1)^{p_i}] = \frac{1}{N} \sum_{j=0}^{N-1} (-1)^{b_{j,m}} \tag{17}$$

Using eqn. (17), EACF of $\{p_i\}$ can be calculated by the next equation.

$$E[\phi_{pp}(\tau)] = \frac{1}{L \cdot N^2} \sum_{i=0}^{L-1} \sum_{j=0}^{N-1} \sum_{\sigma=0}^{N-1} (-1)^{b_{j,m}} \cdot (-1)^{b_{\sigma,m+\mu}} \tag{18}$$

Here, μ is equal to $(\bmod\ \tau, k)$. From eqn. (18), if eqn. (17) is equal to 0, EACF of $\{p_i\}$ becomes 0 and the generated binary random sequence $\{p_i\}$ have good randomness properties. In order to satisfy that eqn. (17) is equal to 0 for each m $(0 \leq m \leq k-1)$, the binary sequence $\{b_{i,m}\}$ $i = 0, 1, \cdots N-1)$ must include 1 and 0 equally in a period N. Then, the maximum value of b_j becomes

$$P - 1 = \max b_j = \sum_{j=0}^{k-1} 2^j = 2^k - 1$$

$$P = 2^k \tag{19}$$

If eqn. (19) is satisfied, eqn. (17) is equal to 0 and consequently, EACF of $\{p_i\}$ becomes

$$E[\phi_{qq}(\tau)] = 0$$

(ii) In case of $1 \leq \tau \leq k-1$, if the delay τ is smaller than $k - m$, the i-th and the $(i+\tau)$-th element of $\{p_i\}$ are sampled from the same element of the multi-valued sequence $\{b_i\}$. Then, each term of the right-hand side of the eqn. (16) is given by the next equation.

$$\begin{aligned} &E[(-1)^{p_i} \cdot (-1)^{p_{i+\tau}}] \\ &= \frac{\tau}{N^2 \cdot k} \sum_{m=k-\tau}^{k-1} \sum_{j=0}^{N-1} \sum_{\sigma=0}^{N-1} (-1)^{b_{j,m}} \cdot (-1)^{b_{\sigma,m+\tau}} \\ &\quad + \frac{k-\tau}{N \cdot k} \sum_{m=0}^{k-\tau-1} \sum_{j=0}^{N-1} (-1)^{b_{j,m}} \cdot (-1)^{b_{j,m+\tau}} \end{aligned}$$

When eqn. (19) is satisfied, the first and the second term of the right-hand side of this equation are equal to 0. Then, EACF of the binary random sequence $\{p_i\}$ becomes

$$E[\phi_{pp}(\tau)] = 0$$

and the generated binary random sequence have best randomness.

4. Computer simulation

In order to show that good binary sequences can be generated by use of the proposed method, computer simulations are carried out. In this paper, the uniform random numbers used in method A and B are generated by a high-order M-sequence [5] and distribute uniformly in a high-dimensional space.

The randomness of the binary random sequences $\{q_i\}$ generated by method A is evaluated by use of the concept called merit factor Fr [3] which is defined by the next equation.

$$Fr = \frac{1}{2\sum_{\tau=1}^{M}(E[\phi_{qq}(\tau)])^2} \tag{20}$$

For the calculation of the merit factor Fr, the ensemble averaged ACF of the binary random sequence $\{q_i\}$ is used instead of EACF of $\{q_i\}$. Here, the averaging number is equal to 500,000 and the maximum delay M is equal to 64.

In Fig.2, maximum and minimum values of the merit factor Fr of the binary random sequence $\{q_i\}$ are plotted where the period N of the original binary sequence is equal to 24. When the tuple length k is shorter than 10, the maximum value of the merit factor Fr takes large value and the generated binary random sequence $\{q_i\}$ have good randomness properties. On the other hand, the minimum value of Fr becomes smaller as the tuple length becomes longer. It is shown that good binary random sequences can not always be obtained by the method A even if uniform random numbers have good randomness properties.

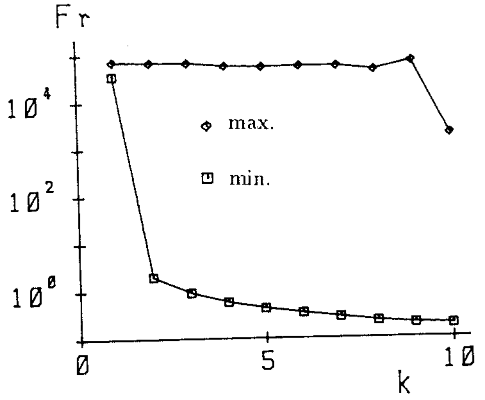


Fig.2 Maximum and minimum values of the merit factor Fr of binary random sequence $\{q_i\}$

In order to generate good binary random sequences by use of method A, the original binary sequence $\{a_i\}$ must satisfy eqn. (16). Then, the probability Pr that the generated binary random sequences have good randomness properties can be calculated by the next equation.

$$Pr = \frac{\text{number of } \{a_i\} \text{ satisfying eqn. (14)}}{J}$$

Here, J is a number of binary sequence $\{a_i\}$ satisfying the condition ii. In this paper, when the period N of $\{a_i\}$ is shoter than 28, all of the binary sequence are used to calculated the probability Pr. When the period N becomes long, the number of the binary sequence $\{a_i\}$ which satisfy the condition ii becomes very large. When N is longer than 24, we choose 1,000,000 different binary sequences randomly to calculate the probability Pr. Then, the number J is given by the next equation.

$$J = \begin{cases} {}_N C_{N/2} & (N \leq 24) \\ 1,000,000 & (N \geq 28) \end{cases}$$

The relation between the probability Pr and the period N are shown in Fig.3. From this figure, it is shown that the longer the period of the binary sequence $\{a_i\}$, the samller the probability Pr. It is also shown that when the tuple length k becomes long, the probability Pr becomes small rapidly.

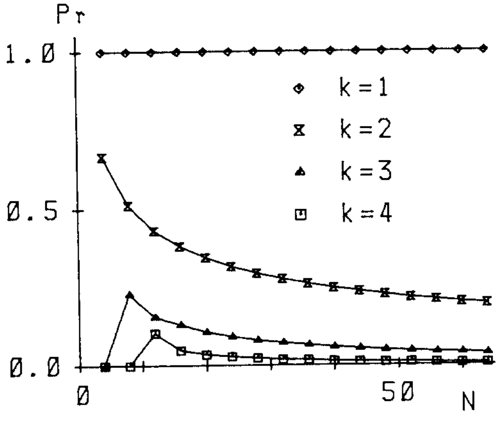


Fig.3 Probability Pr vs. period N of the original binary sequence $\{a_i\}$

In Fig.4, maximum and minimum values of Fr obtained from the binary random sequences generated by method B are plotted. Here, the value P satisfy eqn. (19) and the period N of the P-valued sequence is equal to 2^k. Comparing Fig.2 and Fig.4, the minimum values of Fr calculated from the binary random sequences generated by method B take large values. So, good binary random sequences can always be obtained by method B if eqn. (19) is satisfied.

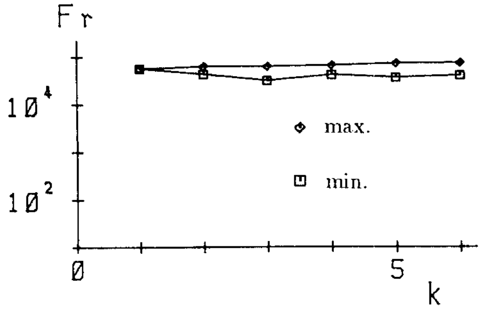


Fig.4 Maximum and minimum values of the merit factor Fr of binary random sequence $\{p_i\}$

The maximum number k_m of elements which can be generated from one uniform random number is shown in Fig.5. From Fig.5, it is shown that the number k_m obtained by method A is always larger than that obtained by method B. Therefore, binary random sequences can be generated more rapidly by use of method A.

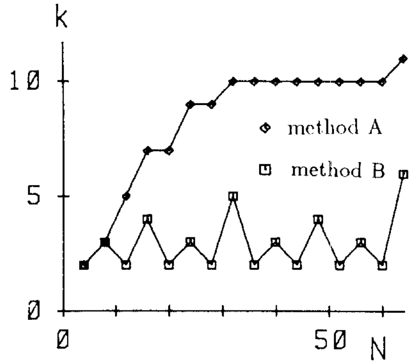


Fig.5 Maximum number of elements vs. period of the original binary sequence $\{a_i\}$

5. Conclusion

In this paper, two methods called method A and method B are proposed for fast generation of binary random sequences. The methods are both based on the random sampling method. In method A, binary random sequences are generated by use of k-tuples of a binary sequence $\{a_i\}$ and uniform random numbers. Expected values of autocorrelation function of the binary random sequence generated by method A are derived theoretically. From the theoretical values, the optimum condition for obtaining ideal binary random sequences is introduced.

In method B, a P-valued sequence is used instead of a binary sequence. It is shown that when the value P is equal to 2^k, the binary random sequences generated by method B have good randomness properties.

References

1. H.Harada, H.Kashiwagi, S.Honda and K.Oguri: On Correlation Function of Randomly Sampled M-sequence, Trans. SICE, **23**-11, 1145/1150 (1987) (in Japanese)
2. H.Harada, H.Kashiwagi, S.Honda and K.Oguri: Binary Random Sequence Generation by Use of Randomly Sampled M-sequence, Proc. '87 KACC, 832/835 (1987)
3. H.Harada, H.Kashiwagi and T.Takada: Evaluation of Randomness of Binary Random Sequence, Proc. '89 KACC, 979/983 (1989)
4. F. J. McWilliams and N. J. A. Sloane: Pseudo-Random Sequences and Arrays, Proc. IEEE, **64**-12, 1715/1729 (1976)
5. H.Harada and H.Kashiwagi: Random Number Generation by Use of M-Sequence, Trans. SICE, **23**-8, 806/811 (1987) (in Japanese)