'89 KACC 1989. 10. 27~28

Evaluation of Randomness of Binary Random Sequence

*Hiroshi Harada**, *Hiroshi Kashiwagi**, *Tadashi Takada***

* *Faculty of Engineering, Kumamoto University, Kumamoto, Japan*
** *Nippon Electric Company, 1-10, Nisshin-chou, Fuchu, Japan*

Abstract: This paper proposes a new concept, called merit factor Fr, for evaluating the randomness of binary random sequences. The merit factor Fr is obtained from the expected values of the autocorrelation function of the binary random sequence. Using this merit factor Fr, randomness of the binary random sequences generated by the random sampling method is evaluated.

1. Introduction

Binary random sequences are widely used as the modulation codes for continuous wave radar or spread-spectrum communication system. A new method has been proposed by the authors for generation of the binary random sequences based on an M-sequence [1,2,3]. This method is called random sampling method and the binary random sequences are generated by use of successive k-tuples of an M-sequence and uniform random numbers. The authors showed that the expected values of the autocorrelation function (ACF) of the generated binary random sequence can be calculated theoretically. However, the optimum condition is not yet given for obatining binary random sequence having good random properties.

In this paper, a new concept, called merit factor Fr, for evaluating the randomness of binary random sequence is proposed. Using the merit factor Fr, randomness of the binary random sequences generated by the random sampling method is evaluated, and the optimum condition for generation of the binary random sequence is introduced.

2. Evaluation of randomness of binary random sequence based on autocorrelation function

When binary random sequence is used as the modulaton codes, it is desirable that the ACF of the binary random sequence has sharp peak at delay 0, while at the other delays ACF is almost equal to 0, just like δ-function.

Let $\{\alpha_i\}$ denote a binary random sequence and L be the period of $\{\alpha_i\}$.

$$\{\alpha_i\} = \alpha_0, \alpha_1, \cdots, \alpha_{L-1} \quad (\alpha_i = \pm 1)$$

Golay proposed the concept, called merit factor F, for evaluating the randomness of binary random sequences [4]. The merir factor F is defined by the next equation.

$$F = \frac{L^2}{2\sum_{i=1}^{L-1}\gamma_i^2} \tag{1}$$

Here, γ_i is given as,

$$\gamma_i = \sum_{j=i+1}^{L} \alpha_j \cdot \alpha_{j-i} \tag{2}$$

The ACF of $\{\alpha_i\}$ is defined by eqn. (3).

$$\phi_{\alpha\alpha}(i) = \frac{1}{L-i}\sum_{j=i+1}^{L} \alpha_j \cdot \alpha_{j-i} \tag{3}$$

Substituting eqn. (3) into eqn. (2), γ_i can be expressed by the ACF of $\{\alpha_i\}$ as,

$$\gamma_i = (L-i)\phi_{\alpha\alpha}(i) \tag{4}$$

Using eqns. (1) and (4), the merit factor F is defined by the next equation.

$$F = \frac{1}{2\sum_{i=1}^{L-1}(1-\frac{i}{L})^2\phi_{\alpha\alpha}^2(i)} \tag{5}$$

From eqn. (5), if the binary sequence $\{\alpha_i\}$ has good randomness, ACF of $\{\alpha_i\}$ is almost equal to 0, then the merit factor F takes large value. While, when the binary sequence is not good binary random sequence, the merit factor becomes small. So, the randomness of the binary sequence can be evaluated by the merit factor F.

In this paper, a new concept is proposed for evaluating the randomness of the binary random sequence. The new concept, called merit factor Fr, is defined by the next equation.

$$Fr = \frac{1}{2\sum_{\tau}^{N}{}_{1}(E[\phi_{rr}(\tau)])^2} \tag{6}$$

Here, $E[\phi_{rr}(\tau)]$ is the expected values of ACF (EACF) of the binary random sequence $\{r_i\}$ and N is the period of the original M-sequence. Comparing, eqn. (5) and (6), the denominator of the right side of eqn. (5) is the weighted summation of the ACF of binary random sequence, while that of eqn. (6) is the equally weighted summation of the EACF of the binary ramdon sequence.

3. Evaluation of randomness of the binary random sequence generated by the random sampling method

In this section, the randomness of the binary random sequence generated by the random sampling method is evaluated by use of the merit factor Fr. The random sampling method in literature [1] is as follows. Let $\{a_i\}$ denote an n-the degree M-sequence and N be the period of $\{a_i\}$

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

$$N = 2^n - 1$$

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

$$a_{ki} = (a_{ki}, a_{ki+1}, \cdots, a_{ki+k-1})$$

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 a_{ki} is chosen. Here, $[k \cdot X_i]$ denotes the maximum integer less than $k \cdot X_i$. Let $\{r_i\}$ be the binary random sequence generated by this method, $\{r_i\}$ can be expressed by the original M-sequence $\{a_i\}$ as

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

ACF of the sequence $\{r_i\}$ is defined [5] as,

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

and the expected values of the ACF (EACF) of the sequence $\{r_i\}$is given as eqn. (7) [1],[2].

$$E[\phi_{rr}(\tau)] = \frac{1}{Nk^2}\sum_{i=0}^{N-1}\sum_{j=0}^{k-1}\sum_{l=0}^{k-1}(-1)^{a_{ki+j}} \cdot (-1)^{a_{k(i+\tau)+l}} \tag{7}$$

When the tuple length k and the period N of the original M-sequence are coprime each other, the EACF of the binary random sequence $\{r_i\}$ can be calculated theoretically [1],[2]. On the other hand, if they are not coprime each other, the EACF of the binary random sequence cannot be expressed as the function of k and N. However, when the tuple length is equal to the period of the M-sequence, EACF of the sequence $\{r_i\}$ can be easily obtained. In this case, substituting eqns. $k = N$, $a_{Ni+j} = a_j, a_{N(i+\tau)+l} = a_l$ into eqn. (7), EACF of the sequence $\{r_i\}$ is derived as

$$E[\phi_{rr}(\tau)] = \frac{1}{N^3}\sum_{i=0}^{N-1}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1}(-1)^{a_j} \cdot (-1)^{a_l}$$

$$= \frac{1}{N^2}\{\sum_{j=0}^{N-1}(-1)^{a_j}\}^2 \tag{8}$$

Since $\{a_i\}$ is an n-th degree M-sequence, the number of 1's in a period of $\{a_i\}$ is equal to 2^{n-1} and that of 0's is equal to $2^{n-1} - 1$ [6]. Then, the summation of $(-1)^{a_j}$ becomes

$$\sum_{j=0}^{N-1}(-1)^{a_j} = -2^{n-1} + 2^{n-1} - 1 = -1 \tag{9}$$

Substitution eqn. (9) into eqn. (8) yields

$$E[\phi_{rr}(\tau)] = \frac{1}{N^2}$$

Theoretical values of the merit factor Fr can be calculated using EACF of the binary random sequence $\{r_i\}$. And it is shown that when the tuple length is equal to the period of the original M-sequence, the merit factor Fr takes the maximum value

$$Fr = \frac{1}{2\sum_{r=1}^{N}\frac{1}{N^3}} = \frac{N^3}{2}$$

and the binary random sequence $\{r_i\}$ becomes most random.

In order to prove that the theoretical values of Fr are correct, computer simulation is carried out, and the result is shown in Fig. 1.

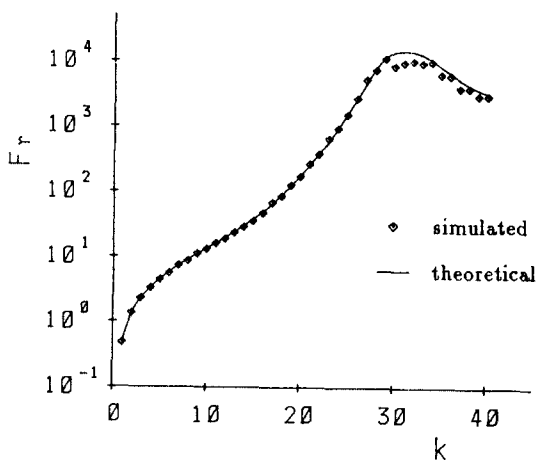


Fig. 1 Merit factor Fr vs. tuple length k when the characteristic polynomial of M-sequence is $f(x) = x^5 + x^2 + 1$

In Fig. 1, the merit factor Fr obtained from the ensemble averaged ACF of the binary random sequence $\{r_i\}$ are plotted, where the averaging number is 100,000 and the characteristic polynomial of the original M-sequence is

$$f(x) = x^5 + x^2 + 1$$

A solid line in Fig. 1 is the theoretical values of the merit factor Fr calculated from EACF of the sequence $\{r_i\}$. From Fig. 1, it is shown that when the tuple length k is less than 29, there is little difference between the simulated values and the theoretical values. While, when k is greater than 30, the difference becomes large. However, it is considered that the difference becomes small when the averaging number increases.

From the result of the computer simulation, it is shown that the optimum condition for obtaining ideal binary random sequence by the random sampling method is to choose the tuple length to be equal to the period of the original M-sequence. In this case, the binary random sequence is expressed as

$$\{r_i\} = a_{[N \cdot X_0]}, a_{[N \cdot X_1]}, \cdots, a_{[N \cdot X_i]}, \cdots$$

The example of the ensemble averaged ACF of the binary random sequence generated on the optimum condition is shown in Fig. 2.

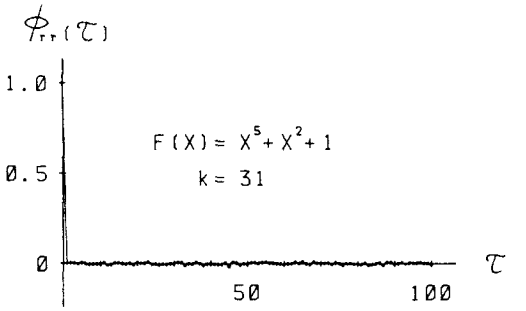


Fig. 2 Ensemble averaged ACF of binary random sequence generated by the random sampling method

Here, the characteristic polynomail is the same as that in Fig. 1 and the averaging number is 1,000. It is clear that the obtained ensemble averaged ACF of the sequence $\{r_i\}$ is almost equal to δ-function. So, it is shown that the generated binary random sequences have good random properties.

4. Evaluation of randomness of binary random sequence obtained from an arbitrary binary sequence

When an arbitrary binary sequence is used as the original binary sequence instead of an M-sequence, binary random sequences can be also generated by the random sampling method. Let $\{q_i\}$ denote an arbitrary binary sequence

$$\{q_i\} = q_0, q_1, \cdots, q_{L-1} \quad (q_i = 0 \text{ or } 1)$$

Here, L is the period of $\{q_i\}$. Let $\{p_i\}$ be the binary random sequence obtained from $\{q_i\}$ by the random sampling method mentioned in section 3. Then, $\{p_i\}$ can be also expressed by the original binary sequence $\{q_i\}$ as

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

where k is the tuple length and X_i $(i = 0, 1, \cdots)$ is a random number distributed uniformly between 0 and 1. In this case, EACF of $\{p_i\}$ is given by eqn. (10).

$$E[\phi_{pp}(\tau)] = \frac{1}{Lk^2}\sum_{i=0}^{L-1}\sum_{j=0}^{k-1}\sum_{l=0}^{k-1}(-1)^{q_{ki+j}} \cdot(-1)^{q_{k(i+\tau)+l}} \quad (10)$$

Since the properties of the binary sequence $\{q_{ki}\}$, which is obtained by sampling every k digit of the binary sequence $\{q_i\}$, is not yet known, it is difficult to express the EACF of the binary random sequence $\{p_i\}$ as the function of the tuple length and the period of the original binary sequence.

However, when the tuple length is equal to the period of $\{q_i\}$, EACF of the binary random sequence $\{p_i\}$ can be easily obtained. Substitution of eqns. $k = L, q_{Li+j} = q_j, q_{L(i+\tau)+l} = q_l$ into eqn. (10) yields

$$E[\phi_{pp}(\tau)] = \frac{1}{L^3}\sum_{i=0}^{L-1}\sum_{j=0}^{L-1}\sum_{l=0}^{L-1}(-1)^{q_j} \cdot(-1)^{q_l}$$

$$= \frac{1}{L^2}\{\sum_{j=0}^{L-1}(-1)^{q_j}\}^2$$

Let c_1 be the number of 1's in a period of the sequence $\{q_i\}$ and c_0 be that of 0's. Then, EACF of $\{p_i\}$ becomes

$$E[\phi_{pp}(\tau)] = (\frac{c_1 - c_0}{L})^2 \quad (11)$$

If the number of 1's in a period of the sequence $\{q_i\}$ is equal to that of 0's, substitution of $c_1 = c_0$ into eqn. (11) yields

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

Consequently, the merit factor Fr becomes

$$Fr = \infty$$

and the generated binary random sequence shows the most randomness.

A computer simulation is carried out and the result is shown in Fig. 4. In this case, the original binary sequence is an n-th degree de Bruijn sequence [7]. The characteristic polynomial of the de Bruijn sequence $\{q_i\}$ is the same polynomial used in Fig. 1 and the period of $\{q_i\}$ is $L = 32$. In Fig. 3, the merit factor Fr obtained from the ensemble averaged ACF of the binary random sequence $\{p_i\}$ are plotted, where the averaging number is 100,000. The solid line in Fig. 3 is also the theoretical values

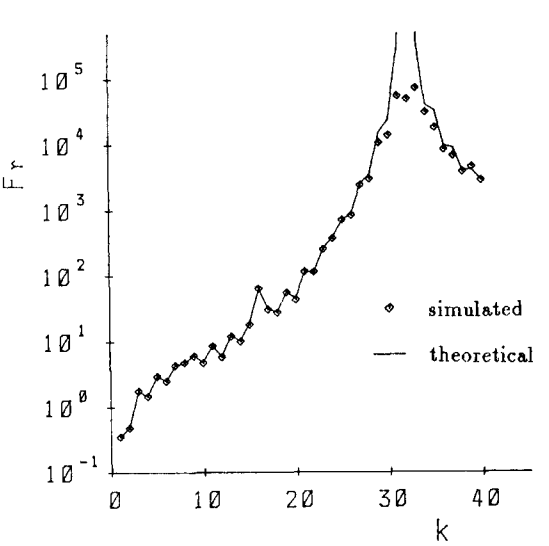
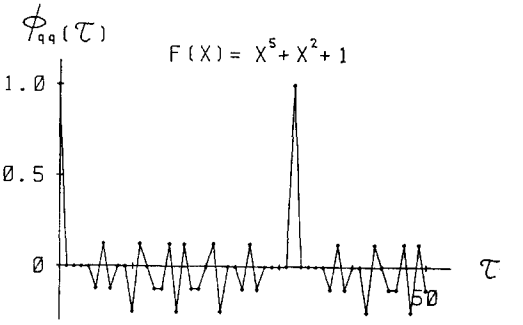
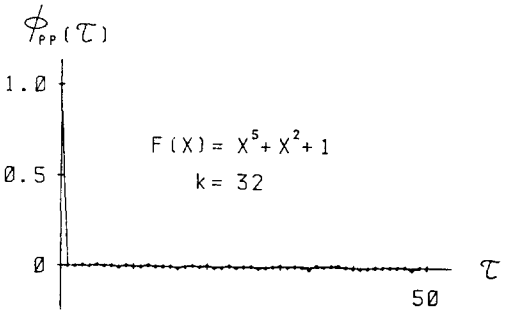


Fig. 3 Merit factor Fr vs. tuple length k when the characteristic polynomial of de Bruijn sequence is $f(x) = x^5 + x^2 + 1$



(a) ACF of $\{q_i\}$



(b) ensemble averaged ACF of $\{p_i\}$

Fig. 4 ACF of de Bruijn sequence $\{q_i\}$ and ensemble averaged ACF of binary random sequence $\{p_i\}$

of Fr. A de Bruijn sequence can be generated by adding one 0 to the longest run of 0 in a period of an M-sequence [7]. So the number of 1's in a period of an n-th degree de Bruijn sequence and that of 0's are equal.

From Fig. 3, when the tuple length is equal to the period of the de Bruijn sequence, the theoretical value of the merit factor Fr becomes infinite and the simulated value of Fr takes maximum value. Comparing Fig. 3 with Fig. 1, the maximum value of the merit factor Fr in Fig. 3 is about 10 times as large as that in Fig. 1, though the period of the de Bruijn sequence used in Fig. 3 is almost equal to that of the M-sequence used in Fig. 1. So, when the tuple length is equal to the period of the de Bruijn sequence, the generated binary random sequence has more randomness compared with the binary random sequence obtained from the M-sequence.

ACF of the de Bruijn sequence $\{q_i\}$ used in Fig. 3 and the ensemble averaged ACF of the binary random sequence generated on the optimum condition are shown in Fig. 4 (a) and (b), respectively. Here, the averaging number is 1,000. From Fig. 4(b), it is clear that the ensemble averaged ACF of the binary random sequence is almost equal to δ-function and the generated binary sequence has good randomness.

5. Conclusion

A new concept, called merit factor Fr, is proposed for evaluating the randomness of binary random properties. The merit factor Fr is defined using the expected values of the autocorrelation function of the binary random sequence. Using the merit factor Fr, the randomness of the binary random sequences generated by the random sampling method is evaluated. And it is shown that when the tuple length is equal to the period of the original M-sequence, the merit factor Fr takes the maximum value and the generated binary random sequence has most randomness.

When an arbitrary binary sequence is used as the original binary sequence, the randomness of the binary random sequences generated by the random sampling method is also evaluated. In this case, the optimum conditions for obtaining ideal binary random sequence having good random properties are introduced. The first condition is to choose the tuple length to be equal to the period of the original binary sequence, and the second condition is to use the binary random sequence which includes 1's and 0's equally in a period.

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, S.Honda and K.Oguri: On Some Properties of Randomly Sampled M-sequence, Trans. SICE, **24**-8, 773/778 (1988) (in Japanese)
4. M. J. E. Golay: Sieves for Low Autocorrelation Binary Sequences, IEEE Trans Inf. Theory, **IT-23**-1, 43/61 (1977)
5. F. J. McWilliams and N. J. A. Sloane: Pseudo-Random Sequences and Arrays, Proc. IEEE **64**-12, 1715/1729 (1976)
6. H.Kashiwagi : Recent Topics on M-sequence, Journal of SICE, **20**-2, 236/245 (1981) (in Japanese)
7. G.Hoffmann de Visme: Binary Sequences, English Universities Press, (1971)