'90 KACC 1990. 10. 26~27

On Desirable Conditions for a Random Number Used in the Random Sampling Method

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

* *Faculty of Engineering, Kumamoto University, Kumamoto, Japan*
** *NEC Corporation, 1-10, Nisshin-chou, Fuchu, Japan*

Abstract: A new method called random sampling method has been proposed for generation of binary random sequences. In this paper, a new concept, called merit factor Fn, is proposed for evaluating the randomness of the binary random sequences generated by the random sampling method. Using this merit factor Fn, some desirable conditions are investigated for uniform random numbers used in the random sampling method.

1. Introduction

Binary random sequences are widely used as the modulation codes for continuous wave radar or spread-spectrum communication system. For generation of the binary random sequences a new method was proposed by the authors [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 arbitrary binary sequence and uniform random numbers. The optimum conditions for obtaining ideal binary random sequences having good random properties were introduced [4]. 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 sequence which includes 1's and 0's equally in a period.

As for the conditions for the uniform random numbers, it is only pointed out that each element of the uniform random number sequence must be independent [1],[2]. However, it is difficult, in general, to generate artificially uniform random numbers which are truly independent each other.

In this paper, a new concept is proposed for the evaluation of the randomness of the binary random sequence. And using this concept, the authors show desirable conditions for uniform random numbers used in the random sampling method.

2. Evaluation of randomness of binary random sequence

Let us briefly review the random sampling method and the merit factor Fr proposed in reference [4]. Let $\{a_i\}$ denote an arbitrary binary sequence and N be the period of $\{a_i\}$

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

The random sampling method is as follows. First, 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 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 [5] as,

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

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

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

When the tuple length k is equal to the period N of the original binary sequence,

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

Substituting these equations into eqn. (1), the EACF of the binary random sequence $\{r_i\}$ is given by next equation.

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

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.

For the evaluation of the randomness of the binary random sequence, the authors proposed a new concept based on the EACF of the binary random sequence [4]. This concept is called merit factor Fr which is defined by the next equation.

$$Fr = \frac{1}{2\sum_{\tau=1}^{L}(E[\phi_{rr}(\tau)])^2} \tag{3}$$

From eqn.(3), when the binary random sequence $\{r_i\}$ has good randomness, EACF of $\{r_i\}$ is almost equal to 0, then the merit factor Fr takes large value. While, when the binary random sequence is not a good random sequence, the merit factor becomes small. So, the randomness of the sequence $\{r_i\}$ can be evaluated by the merit factor Fr. 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.(2) yields

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

Consequently, the merit factor Fr becomes

$$Fr = \infty$$

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

In this paper, another new concept is proposed for the evaluation of the randomness of the binary random sequence. First, another binary sequence $\{q_i\}$ is derived from the binary random sequence $\{r_i\}$. The i-th element of $\{q_i\}$ is defined as

$$q_i = r_i \oplus r_{i+1} \tag{4}$$

Here, $\oplus$ denotes exclusive-OR operation. When a run continues in the sequence $\{r_i\}$, r_i is equal to r_{i+1}, meaning q_i is equal to 0. At the end of the run, r_i is not equal to r_{i+1}, so q_i is equal to 1. It is considered that the randomess of runs of the binary random sequence $\{r_i\}$ influences the randomness of binary sequence $\{q_i\}$.

ACF of $\{q_i\}$ is also defined as

$$\phi_{qq}(\tau) = \frac{1}{L}\sum_{i=0}^{L-1}(-1)^{q_i}\cdot(-1)^{q_{i+\tau}} \tag{5}$$

Taking expectation of both sides of eqn.(5), EACF of $\{q_i\}$ is given as

$$\begin{aligned} E[\phi_{qq}(\tau)] &= E[\frac{1}{L}\sum_{i=0}^{L-1}(-1)^{q_i}\cdot(-1)^{q_{i+\tau}}] \\ &= \frac{1}{L}\sum_{i=0}^{L-1}E[(-1)^{q_i}\cdot(-1)^{q_{i+\tau}}] \\ &= \frac{1}{L}\sum_{i=0}^{L-1}E[(-1)^{r_i}\cdot(-1)^{r_{i+1}} \\ &\qquad \cdot(-1)^{r_{i+\tau}}\cdot(-1)^{r_{i+\tau+1}}] \end{aligned}$$

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

$$E[\phi_{qq}(\tau)] = (\frac{c_1 - c_0}{N})^4 \tag{6}$$

Here, c_1 is also the number of 1's in a period of the original sequence and c_0 is that of 0's. From eqn. (6), if c_1 is equal to c_0, the EACF of $\{q_i\}$ becomes

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

By use of EACF of $\{q_i\}$, a new concept is derived for evaluating the randomness of the binary random sequence. Using EACF of the sequence $\{q_i\}$ instead of that of $\{r_i\}$, another merit factor Fn is defined by the next equation.

$$Fn = \frac{1}{2\sum_{\tau=1}^{L}(E[\phi_{qq}(\tau)])^2} \tag{7}$$

When the binary random sequence $\{r_i\}$ has good randomness, the binary random sequence $\{q_i\}$ also becomes a good random sequence. Consequently, the merit factor Fr and Fn both take large values.

3. Computer simulation

In this section, in order to show the desirable conditions for the uniform random number (URN) sequence used in the random sampling method, binary random sequences are generated by the random sampling method using various URN sequences. The randomness of the generated binary random sequence is evaluated by the merit factor Fr and Fn.

In this paper URN sequences generated by 3 methods are used. The recurrence equations are shown in Table 1. Here, $\{X_i\}$ is a URN sequence. $\{U_i\}$ is an integer sequence and $\{Z_i\}$ is a real number sequence. In method A, URN is generated by a high-order M-sequence [6]. Method B is called Uniform Random Numerator [7] and method C is called Chebyshev mixing method [8]. Some statistical tests are applied to these uniform random numbers and the results are shown in Table 2. The numbers in Table 2 represent the rejected rate among Kolmogorov-Smirnov test (K-S test) [9] repeated 500 times. In this case, the significance level is 5%, so if the URN sequence has good randomness, the numbers in Table 2 are near to 5. From this point of view, URN generated by method A has good ramdonness. URN generated by method B distributes uniformly in one-dimensional space, but the distributions in a high-dimensional space are not uniform. URN generated by method C does not distribute uniformly even in one-dimensional space.

In this paper, an n-the degree de Bruijn sequence is used as the original binary sequence $\{a_i\}$. An n-th degree de Bruijn sequnece is generated by adding one 0 to the longest run of 0's in a period of an n-th degree M-sequence [10]. Then, the period of the de Bruijn sequence is given as

$$N = 2^n$$

The number of 1's in a period of the de Bruijn sequence and that of 0's become

Table 1 Methods of generating uniform random numbers

Method	Recurrence equation
A	$U_i = U_{i-89} \oplus U_{i-88} \oplus U_{i-77} \oplus U_{i-57}$ $X_i = U_i/2^{16}$
B	$U_i = \begin{cases} U_{i-1} + U_{i-2} + U_{i-3} + 1357 & (U_{i-2} < 5 \times 10^7) \\ U_{i-1} + U_{i-2} + U_{i-3} & (U_{i-2} \geq 5 \times 10^7) \end{cases}$ $U_i = U_i \bmod 10^8$ $X_i = U_i/10^8$
C	$Z_i = Z_{i-1}^2 - 2 \quad (-2 < Z_0 < 2)$ $X_i = \cos^{-1}(Z_i/2)/\pi$

Table 2 Results of K-S test

Test / $\{X_i\}$	Frequency	Serial (2nd)	Serial (3rd)	Combination	Run (Above/Below)	Run (Up/Down)	Poker
A	5.2	4.6	6.0	6.6	5.6	6.2	4.2
B	6.2	32.8	4.4	6.4	100.0	100.0	100.0
C	88.0	100.0	100.0	100.0	5.4	100.0	100.0

$$c_1 = c_0 = 2^{n-1}$$

Therefeore, if the URN used in the random sampling method has good randomness, the theoretical values of the merit factor Fr and Fn become inifinite.

Computer simulations are carried out using URN sequences and de Bruijn sequences. The results are shown in Figs. 1,2,3. In these figures the merit factor Fr and Fn are calculated from the ensemble averaged ACF of the sequnece $\{r_i\}$ and $\{q_i\}$. The averaging number is 50,000 and the maximum delay L is equal to 64. In Fig.1, the URN sequence generated by method A, which has good randomness, is used. It is shown that the merit factor Fr and Fn take large values and the binary random sequences have good random properties.

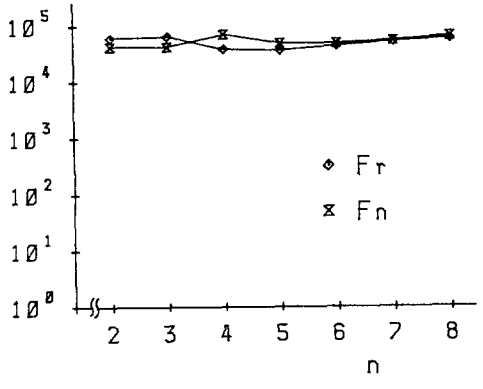

Fig. 1 Merit factor Fr and Fn vs. degree of de Bruijn sequence when URN is generated by method A

URN sequences used in Fig. 2 and Fig.3 are generated by method B and method C, respectively. In Fig.2 , the lower the degree of the de Bruijn sequence, the smaller the merit fctor Fn. On the other hand, in Fig.3 when the degree of the de Bruijn sequence is small, the merit factor Fr and Fn takes large value. From Table 2, the URN generated by method C shows good ramdom property only in the run(Above/Below) test. While result of the run(Above/Below) test of the URN generated by method B is bad. So, it is considered that the result of the run(Above/Below) test affects the randomness of the binary random sequnece generated by the random sampling method. In

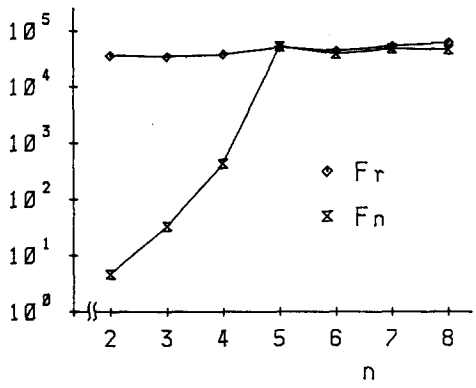

Fig. 2 Merit factor Fr and Fn vs. degree of de Bruijn sequence when URN is generated by method B

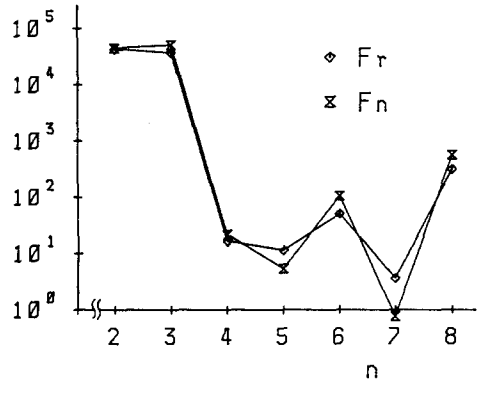

Fig. 3 Merit factor Fr and Fn vs. degree of de Bruijn sequence when URN is generated by method C

order to verify that this hypothesis is correct, a computer simulation is carried out. First, URN sequences which show various randomness in the run(Above/Below) test are generated and the K_{100}^{-} values are obtained from K-S test. Then, using these URN sequences, the binary random sequences are generated by the random sampling method and the merit factor Fn are calculated. The relation between K_{100}^{-} values and the merit factor Fn is shown in Fig.4. It is obvious that the smaller K_{100}^{-} value, the larger the merit factor Fn. When the degree n of the de Bruijn sequence is greater than 5, the merit factor Fn take large values in all cases.

From the results of the computer simulation,

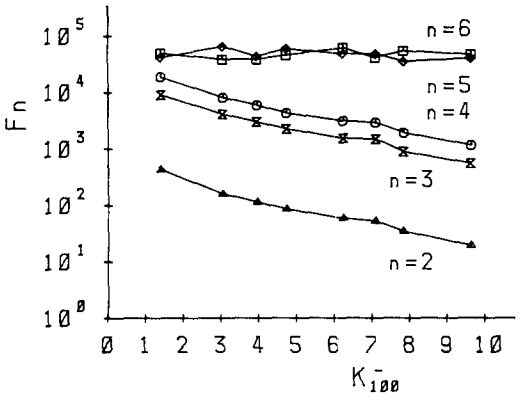

Fig. 4 Merit factor Fn vs. K_{100}^{-} value

the conditions for generating binary good binary random sequence by the random sampling method are as follows.

1. If URN used in the random sampling method has good randomness, binary random sequence having good randomness can be generated from an arbitrary binary sequence.
2. When the distribution of URN are not uniform in high-dimentional space, the degree of the de Bruijn sequence must be high.
3. When URN does not distribute uniformly even in one-dimensional space, good binary random sequence can not obtained by the random sampling method. However, if the URN shows good randomness in run(Above/Below) test and the low degree de Bruijn sequence is used, the generated binary random sequence shows good randomness.

4. Conclusion

A new concept, called merit factor Fn, is proposed for evaluating the randomness of binary random properties. The merit factor Fn is defined using the expected values of the autocorrelation function of the binary random sequence. Using the merit factor Fn, the randomness of the binary random sequences generated by the random sampling method is evaluated. And it is shown that the unifrom random numbers used in the random sampling method must distribute uniformly in high-dimesnionnal space.

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. H.Harada, H.Kashiwagi and T.Takada: Evaluation of Randomness of Binary Random Sequence, Proc. '89 KACC, 979/983 (1989)
5. F. J. McWilliams and N. J. A. Sloane: Pseudo-Random Sequences and Arrays, Proc. IEEE **64**-12, 1715/1729 (1976)
6. H.Harada and H.Kashiwagi: Random Number Generation by Use of M-Sequence, Trans. SICE, **23**-8, 806/811, (1987) (in Japanese)
7. C.G.Swain and M.S.Swain: A Uniform Random Generator that is Reproducible Hardware-independent and Fast, J. Chem. Inf. Sci., **20**-1, 56/58 (1980)
8. R.S.Wikramaratna: ACORN - A New Method for Generating Sequences of Uniformly Distributed Pseudo-random Numbers, J. Comput. Phys., **83** 16/31 (1989)
9. D.E.Knuth: The Art of Computer Programming Vol.2 Seminumerical Algorithms, Addison-Wesley (1981)
10. G.Hoffmann de Visme: Binary Sequences, English Universities Press, (1971)