'87 KACC 1987.10.16～17

Binary Random Sequence Generation by Use of Random Sampling of M-sequence

Hiroshi Harada*, Hiroshi Kashiwagi*, Satoshi Honda* and Kazuo Oguri**

* Faculty of Engineering, Kumamoto University, Kumamoto, 860 Japan
** Nippon Electric Company, 1-10 Nisshin-chou, Fuchu, 183 Japan

Abstract: This paper proposes a new method of generating binary random sequences using a randomly sampled M-sequence. In this paper two methods of sampling are proposed. Expected values of the autocorrelation function of the sequence generated by these methods are calculated theoretically. From the results of computer simulation, it is shown that using these methods, we can get binary random sequences which have good random properties.

1. Introduction

Binary random sequences are used as modulation codes for continuous wave radar or spread-spectrum communication. In these cases, it is required for the sequences to have the following properties.

(i) Autocorrelation function (ACF) of the sequence has a sharp peak at delay 0, while at the other delays ACF is almost equal to 0.

(ii) The number of 1's in the sequence is almost equal to that of 0's.

An M-sequence is often used as a binary random sequence, since it satisfies these properties and can be generated easily by a linear feedback shift register. However, when the stage length of the shift register is short, the generated M-sequence has a short period. In order to generate longer sequences with short stage shift register, some sequences with nonlinear feedback have been proposed [1, 2, 3]. But the properties of those sequences are not well known [1], and the sidelobes of ACF of the sequences are larger than those of M-sequence [2, 3].

In this paper, a new method is proposed for generating binary random sequences using a shift register with short stage. The method is to sample M-sequence randomly [4, 5]. Two random sampling methods are proposed and the expected values of the ACF of the generated sequence are calculated theoretically.

2. Random sampling of M-sequence in case of constant tuple length

Let $\{a_i\}$ denote an n-th degree M-sequence and N be the period of $\{a_i\}$.

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

$$N = 2^n - 1$$

The random sampling method, called method I, is as follows. First, successive k-tuple of $\{a_i\}$ is generated. The k-tuple $\boldsymbol{a}_{ki}$ is given by eqn.(1),

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

where ^{T} denotes transposition. Then, using a random number X_i (i=0,1,2,----), which is distributed uniformly between 0 and 1, $([k \cdot X_i]+1)$'th bit of $\boldsymbol{a}_{ki}$ is chosen. Here, $[k \cdot X_i]$ denotes the maximum integer less than $k \cdot X_i$. Let $\{r_i\}$ denote the sequence generated by method I, then is expressed by $\{a_i\}$ as

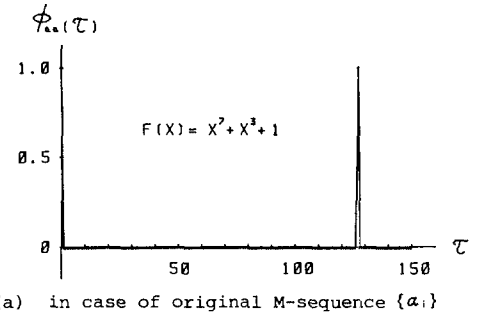
$$\{r_i\} = a_{[k \cdot X_0]}, a_{k+[k \cdot X_1]}, \cdots, a_{ki+[k \cdot X_i]}, \cdots$$

An example of ACF of the original M-sequence $\{a_i\}$ and ACF of the randomly sampled sequence $\{r_i\}$ generated from $\{a_i\}$ are shown in Fig.1(a) and (b), respectively. Here, the characteristic polynomial of $\{a_i\}$ and the tuple length are

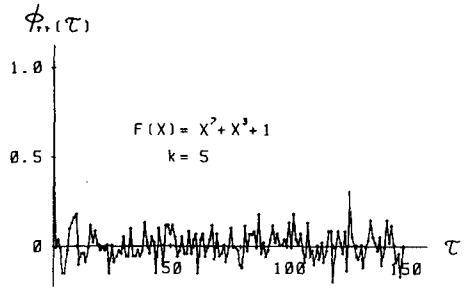
$$f(x) = x^7 + x^3 + 1$$

$$k = 5$$

and the random numbers $\{X_i\}$ are generated by the random number package which has been proposed in literature [6].



(a) in case of original M-sequence $\{a_i\}$



(b) in case of randomly sampled sequence $\{r_i\}$

Fig.1 ACF of $\{a_i\}$ and ACF of $\{r_i\}$ where the characteristic polynomial is $f(x) = x^7 + x^3 + 1$.

In this paper, ACF of binary sequence is defined as follows. First, 1's and 0's in the sequence are replaced by -1's and 1's respectively using next equations.

$$a'_i = (-1)^{a_i} \qquad (i=0,1,2,\cdots)$$

$$r'_i = (-1)^{r_i} \qquad (i=0,1,2,\cdots)$$

Then using a'_i and r'_i, ACF of $\{a_i\}$ and ACF of $\{r_i\}$ are defined by next equations [7].

$$\phi_{aa}(\tau) = \frac{1}{N}\sum_{i=0}^{N-1} a'_i \cdot a'_{i+\tau} = \frac{1}{N}\sum_{i=0}^{N-1} (-1)^{a_i}\cdot(-1)^{a_{i+\tau}}$$

$$= \frac{1}{N}\sum_{i=0}^{N-1} (-1)^{a_i \oplus a_{i+\tau}}$$

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

$$= \frac{1}{N}\sum_{i=0}^{N-1} (-1)^{r_i \oplus r_{i+\tau}} \qquad (2)$$

Here, $\oplus$ means exclusive-OR operation. Comparing Fig.1(b) with (a), $\phi_{aa}(\tau)$ shows a sharp peak at delay N, while $\phi_{rr}(\tau)$ does not show a striking peak. To show the characteristics of $\phi_{rr}(\tau)$, ACF's of $\{r_i\}$ are calculated using 100 different random number sequences, and their ensemble average is shown in Fig.2.

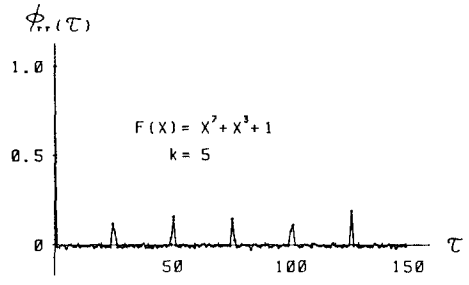


Fig.2 Ensemble averaged ACF of $\{r_i\}$ where the characteristic polynomial is $f(x) = x^7 + x^3 + 1$ and the tuple length is 5.

Here, the characteristic polynomial of the original M-sequence and the tuple length are the same as those in Fig.1(b). Using various characteristic polynomials and tuple lengths, ensemble averaged ACF's of $\{r_i\}$ are calculated and it is shown that they show sharp peaks at delays $\tau = j \cdot N/k$ (j: positive integer).

Theoretical values of the ensemble averaged $\phi_{rr}(\tau)$ are calculated as follows. Taking expectation of both sides of eqn. (2), the expected value of autocorrelation function (EACF) of $\{r_i\}$ is given by

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

$$= \frac{1}{N}\sum_{i=0}^{N-1} E[(-1)^{r_i \oplus r_{i+\tau}}] \qquad (3)$$

Since X_i is a random number having a uniform distribution function between 0 and 1, then

$$Pr\{[k \cdot X_i] = j\} = 1/k \quad (0 \le j \le k-1) \qquad (4)$$

Using eqns. (1) and (4), the probability that r_i is equal to a_{ki+j} is given as

$$Pr\{r_i = a_{ki+j}\} = 1/k \quad (0 \le j \le k-1)$$

Since each element of the random number sequence $\{X_i\}$ is independent, the probability that $r_i \oplus r_{i+\tau}$ is equal to $a_{ki+j} \oplus a_{k(i+\tau)+\ell}$ $(0 \le j, \ell \le k-1)$ is obtained as

$$Pr\{r_i \oplus r_{i+\tau} = a_{ki+j} \oplus a_{k(i+\tau)+\ell}\}$$

$$= Pr\{r_i = a_{ki+j}\} \cdot Pr\{r_{i+\tau} = a_{k(i+\tau)+\ell}\}$$

$$= 1/k^2$$

Therefore, the expected value of $(-1)^{r_i \oplus r_{i+\tau}}$ is given as eqn. (5)

$$E[(-1)^{r_i \oplus r_{i+\tau}}] = \frac{1}{k^2}\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1} (-1)^{a_{ki+j} \oplus a_{k(i+\tau)+\ell}} \qquad (5)$$

Substituting eqn. (5) into eqn. (3), EACF of $\{r_i\}$ is derived as

$$E[\phi_{rr}(\tau)] = \frac{1}{Nk^2}\sum_{i=0}^{N-1}\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1} (-1)^{a_{ki+j} \oplus a_{k(i+\tau)+\ell}} \qquad (6)$$

In this case, if the tuple length and the period of $\{a_i\}$ are relatively prime, $\{a_{ki}\}$ which is the sequence sampled every k digit of $\{a_i\}$, becomes an M-sequence of the same degree [8]. Then, rewriting $\{a_{ki}\} = \{b_i\}$, a_{ki+j} becomes

$$a_{ki+j} = a_{ki+jkd} = a_{k\cdot(i+jd)} = b_{i+jd} \qquad (7)$$

where d is the minimum positive integer satisfying $k \cdot d = 1 \pmod N$ [9]. Using eqn. (7), eqn. (6) is rewritten as

$$E[\phi_{rr}(\tau)] = \frac{1}{Nk^2}\sum_{i=0}^{N-1}\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1} (-1)^{b_{i+jd} \oplus b_{i+\tau+\ell d}}$$

$$= \frac{1}{k^2}\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1} \phi_{bb}(\tau+(\ell-j)d) \qquad (8)$$

Here, $\phi_{bb}(\tau)$ is the ACF of $\{b_i\}$ and since $\{b_i\}$ is an n-th degree M-sequence, $\phi_{bb}(\tau)$ becomes

$$\phi_{bb}(\tau) = \begin{cases} 1 & (\tau = 0 \pmod N) \\ -1/N & (\tau \neq 0 \pmod N) \end{cases} \qquad (9)$$

Using eqns. (8) and (9), EACF of $\{r_i\}$ is calculated as follows.

i) In case of $\tau = s \cdot d$ $(0 \le s \le k-1)$, substitution of $\tau = s \cdot d$ into eqn. (8) yields,

$$E[\phi_{rr}(s \cdot d)] = \frac{1}{k^2}\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1} \phi_{bb}((s+\ell-j)d) \qquad (10)$$

Since d and N are relatively prime, $(s+\ell-j)d$ is equal to 0 (mod N), only when ℓ is equal to j-s. Then, from eqn.(9) $\phi_{bb}((s+\ell-j)d)$ is equal to 1. In other cases, $\phi_{bb}((s+\ell-j)d)$ is equal to $-1/N$, since $(s+\ell-j)d$ is not equal to 0. Therefore, eqn. (10) is rewritten as

$$E[\phi_{rr}(s \cdot d)] = \frac{1}{k^2}\{(k-s) - \frac{1}{N}(k^2-k+s)\}$$

$$= \frac{(N+1)\cdot(k-s) - k^2}{Nk^2} \qquad (11)$$

ii) In case of $\tau = N - s \cdot d$ $(0 \le s \le k-1)$, substitution of $\tau = N - s \cdot d$ into eqn. (8) yields,

$$E[\phi_{rr}(N-s \cdot d)] = \frac{1}{k^2}\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1} \phi_{bb}(N-(\ell-j-s)d)$$

In this case, $\phi_{bb}(N-(\ell-j+s)d)$ is equal to

1 when ℓ is equal to j-s ($s \le j \le k-1$) and $\phi_{bb}(N-(\ell-j+s)d)$ is equal to -1/N when ℓ is not equal to j-s. Then, EACF of $\{r_i\}$ is given by

$$E[\phi_{rr}(N-s\cdot d)] = \frac{(N+1)\cdot(k-s)-k^2}{Nk^2} \qquad (12)$$

iii) In case of $\tau \neq s\cdot d$ or N-s·d ($0 \le s \le k-1$), $\tau+(\ell-j)d$ is never equal to 0 (mod N), then

$$E[\phi_{rr}(\tau)] = \frac{1}{k^2}\cdot\sum_{j=0}^{k-1}\sum_{\ell=0}^{k-1}(-\frac{1}{N}) = -\frac{1}{N}$$

From these results, EACF of $\{r_i\}$ is obtained as a function of the period of the original M-sequence and the tuple length. Substituting s=0 into eqns. (11) and (12), maximum value of EACF of $\{r_i\}$ is given by

$$\max E[\phi_{rr}(\tau)] = E[\phi_{rr}(j\cdot N)] \quad (j=1,2,\cdots)$$

$$= \frac{N-k+1}{Nk} \qquad (13)$$

In order to verify that these theoretical values are correct, a computer simulation is carried out and the results are shown in Fig.3.

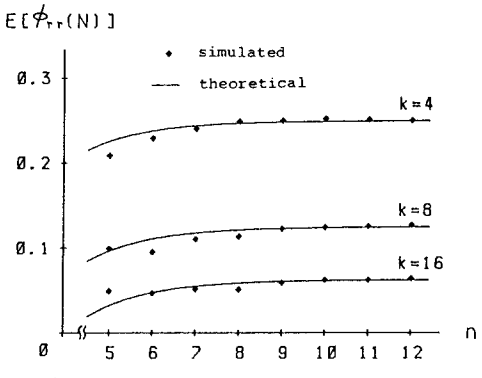


Fig.3 Simulated and theoretical maximum values of ensemble averaged $\{r_i\}$.

In Fig.3, maximum values of the ensemble averaged $\phi_{rr}(\tau)$ are plotted, where the averaging number is 200, and theoretical values are calculated by eqn. (13). It is shown that there is little difference between the simulated values and the theoretical values.

3. Random sampling of M-sequence in case of random tuple length

In this section, a new random sampling method is proposed. The method, called method II, is to sample $([k\cdot X_i]+1)$'th bit from a $([k\cdot X_i]+1)$-tuple of M-sequence, where X_i is also a uniform random number between 0 and 1.

Let $\{q_i\}$ denote the sequence generated by method II, the i-th element of $\{q_i\}$ can be expressed using the original M-sequence $\{a_i\}$ as

$$q_i = a_{j(i)} \qquad (i=0,1,2,\cdots)$$

Since q_i is the $([k\cdot X_i]+1)$'th bit of $([k\cdot X_i]+1)$-tuple of $\{a_i\}$, the subscript j(i) is given by

$$j(i) = j(i-1) + [k\cdot X_i] + 1$$

$$= j(i-2) + [k\cdot X_i] + [k\cdot X_{i-1}] + 2$$

$$\vdots$$

$$= i + \sum_{\ell=0}^{i}[k\cdot X_\ell]$$

Then $\{q_i\}$ can be expressed as follows.

$$\{q_i\} = a_{[k\cdot X_0]},\ a_{1+[k\cdot X_0]+[k\cdot X_1]},\ \cdots,\ a_{i+\sum_{\ell=0}^{i}[k\cdot X_\ell]},\ \cdots$$

An example of ACF of $\{q_i\}$ and the ensemble averaged ACF of $\{q_i\}$ are shown in Fig.4 (a) and (b), respectively. Here, characteristic polynomial of $\{a_i\}$ and the maximum tuple length are the same as those in Fig.1(b).

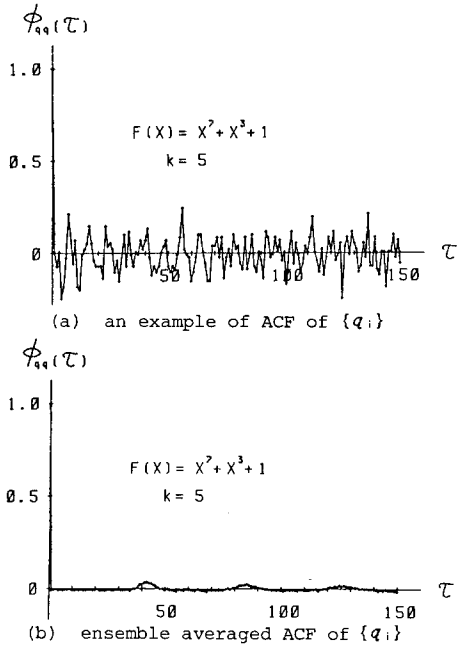


Fig.4 Ensemble averaged ACF of $\{q_i\}$ where the characteristic polynomial is $f(x) = x^7 + x^3 + 1$ and the tuple length is 5.

From Fig.4(b), it is shown that the ensemble averaged ACF of $\{q_i\}$ has broad peaks at delay $\tau = j\cdot\tau_m$ (j:positive integer) and maximum peak value is smaller than that of the ensemble averaged ACF of $\{r_i\}$.

The delay τ_m, where the ensemble averaged ACF of $\{q_i\}$ shows maximum value, is calculated theoretically as follows. Let L_q be the mean length of $\{q_i\}$ which can be generated using N elements of $\{a_i\}$. Then q_i and q_{i+L_q} are obtained by sampling at the same part of $\{a_i\}$. Therefore, when delay is equal to L_q, the ensemble averaged ACF of $\{q_i\}$ shows maximum value. Let j_m be the mean length of $\{a_i\}$, which is necessary for generating one element of $\{q_i\}$, then L_q is given by j_m as

$$L_q = N/j_m \qquad (14)$$

Since X_i is a uniform random number between 0 and 1, j_m is given from eqn. (4) as

$$j_m = E[j(i)-j(i-1)] = \sum_{\ell=0}^{k-1}(\ell+1)\cdot Pr\{[k\cdot X_i]=\ell\}$$

$$= \sum_{\ell=0}^{k-1}\frac{\ell+1}{k} = \frac{k+1}{2} \qquad (15)$$

Substituting eqn. (15) into eqn. (14), the delay τ_m is given by

$$\tau_m = L_q = \frac{2N}{k+1} \tag{16}$$

From the result of computer simulation, it is shown that there is little difference between the observed delays τ_m's and the theoretical delays in eqn. (16).

Maximum value of the ensemble averaged ACF of $\{q_i\}$ is also calculated theoretically as follows. Let A be the number of places where q_i and $q_{i+\tau}$ agree, and D be the number of places where they disagree. Then ACF of $\{q_i\}$ is rewritten as

$$\phi_{qq}(\tau) = \frac{A-D}{N} \tag{17}$$

When delay is not equal to τ_m, A is almost equal to D. Then from eqn.(17), $\phi_{qq}(\tau)$ is equal to 0. However, if delay is equal to τ_m, the probability that j(i) is equal to j(i+ τ_m) becomes large. Therefore, the ensemble averaged ACF of $\{q_i\}$ shows maximum value. In this case, it is assumed that the summation of the probability of j(i)=j(i+ τ_m) is equal to A-D. Then from eqn. (17), the expected value of $\phi_{qq}(\tau_m)$ is given by

$$E[\phi_{qq}(\tau_m)] = \frac{1}{N}\sum_{i=0}^{N-1} Pr\{j(i)=j(i+\tau_m)\}$$

$$= \frac{1}{N}\sum_{i=0}^{N-1}\sum_{\ell=0}^{N-1} Pr\{j(i)=\ell\}\cdot Pr\{j(i+\tau_m)=\ell\}$$

$$= \frac{1}{N}\sum_{i=0}^{N-1}\sum_{\ell=0}^{N-1} (Pr\{j(i)=\ell\})^2 \tag{18}$$

In eqn. (18), the probability of $j(i)=\ell$ is given by next equation,

$$Pr\{j(i)=\ell\} = \frac{1}{k}\sum_{s=0}^{k-1} Pr\{j(i-1)=\ell-s-1 \ (\mathrm{mod}\ N)\}$$

where

$$Pr\{j(0)=\ell\} = \begin{cases} 1/k & (0\le \ell \le k-1) \\ 0 & (k\le \ell \le N-1) \end{cases}$$

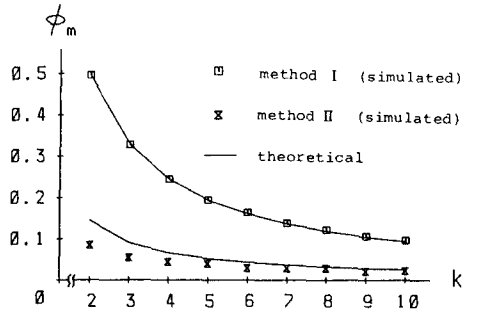


Fig.5 Simulated and theoretical maximum values of EACF of $\{r_i\}$ and $\{q_i\}$ where the characteristic polynomial is $f(x) = x^7 + x^3 + 1$.

A computer simulation is carried out and the result is shown in Fig.5. In Fig.5, the maximum values of the ensemble averaged ACF of $\{r_i\}$ and $\{q_i\}$ are plotted, where the averaging number is 1000 and the characteristic polynomial of the original M-sequence is the same as that in Fig.1. The solid lines in Fig.5 are the theoretical values calculated by eqns. (13) and (18). From Fig.5, it is shown that the theoretical values show good agreement with the simulated values. It is also shown that the maximum values of the ensemble averaged ACF of $\{q_i\}$ are smaller than those of $\{r_i\}$.

4. Conclusion

A new method is proposed for generating binary random sequences using randomly sampled M-sequence. In this paper, two methods of sampling, called method I and method II , are proposed. The EACF of the sequences generated by method I are calculated theoretically. And in case of the sequences generated by method II , the maximum values of the EACF are also calculated theoretically.

Computer simulations are carried out and it is shown that these theoretical values show good agreement with the actual values. It is also shown that the maximum values of the EACF of the sequence generated by method II are smaller than those of the sequence generated by method I . From these results, we see that method II is better than method I in order to get binary random sequences having good random properties.

References

[1] E.L.Key: An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generator, IEEE Trans. Information Theory, IT-22-6, 732/736 (1976)

[2] S.M.Jennings: Autocorrelation Function of the Multiplexd Sequence, IEE Proc. F, Commun. Radar & Signal Processing, 131-2, 169/172 (1984)

[3] J.D. Olsen, R.A.Scholtz and L.R.Welch: Bent Function Sequence, IEEE Trans. Information Theory, IT-28-6,856/864 (1982)

[4] H.Harada, H.Kashiwagi, S.Honda and K.Oguri: On Correlation Function of Randomly Sampled M-sequence, Trans. SICE, 23-11, (1987) (in Japanese)

[5] H.Harada, H.Kashiwagi, S.Honda and K.Oguri: On Some Properties of Randomly Sampled M-sequence, submitted tc Trans. SICE (in Japanese)

[6] H.Harada and H.Kashiwagi: Random Number Generation by Use of M-sequence, Trans. SICE 23-8, (1987) (in Japanese)

[7] F.J.McWilliams and N.J.A.Sloane: Pseudo-Random Sequences and Arrays, Proc. IEEE, 64-12, 1715/1720 (1976)

[8] H.Kashiwagi: Recent Topics on M-sequence, Journal of SICE, 20-2, 236/245, (1981) (in Janapese)

[9] H.Kashiwagi: On Some Properties of TLP Random Numbers Generated by M-Sequence, Trans. SICE, 18-8, 828/832 (1982) (in Japanese)