M 系列をランダムにサンプルして
得られる系列の相関関数†

原 田 博 之*・柏 木 潤*・本 多 敏*・小 栗 一 男**

On Correlation Function of Randomly Sampled M-Sequence

Hiroshi HARADA*, Hiroshi KASHIWAGI*, Satoshi HONDA* and Kazuo OGURI**

When we make a sequence by sampling every s digit of an M-sequence, the properties of the obtained sequence are already known. But the properties of randomly sampled M-sequence are not yet known. This paper describes the properties of the randomly sampled M-sequence.

The random sampling method is as follows. First, successive k -tuple of an M-sequence is generated and then using uniform random number $X_i (0 \leq X_i < 1)$, $([k \cdot X_i] + 1)$ 'th digit of the k -tuple is chosen.

Autocorrelation function of the original M-sequence has a sharp peak at delay N (N : period of M-sequence), while ensemble averaged autocorrelation functions of the randomly sampled sequences have small peaks at several delays other than N . Mean values of the autocorrelation functions of the sequences are obtained theoretically as a function of the period of M-sequence and tuple length.

Maximum values of the ensemble averaged crosscorrelation functions between the randomly sampled sequences are also obtained theoretically and it is shown that these values are less than the maximum values of crosscorrelation functions between the original M-sequences.

Key Words: M-sequence, binary sequence, autocorrelation function, crosscorrelation function

1. ま え が き

2 値ランダム系列は CW (Continuous Wave) レーダやスペクトラム拡散通信の変調用符号などに用いられている。M 系列は、この 2 値ランダム系列としてよく用いられるものの一つであり、その統計的性質はくわしく研究されている。特に、自己相関関数が鋭いピークをもつ、系列中の 1, 0 の個数がほぼ等しい、シフトレジスタと Exclusive-OR (排他的論理和) によって簡単に発生できるなどの利点を有している。ところが、M 系列の次数が低い場合には、系列の長さが短くなり、発生できる M 系列の種類も少なくなる。すなわち、M 系列の次数 (シフトレジスタの段数) を n とするとき、その周期 N は

$$N = 2^n - 1$$

で与えられ、発生できる M 系列の種類はその次数の原始多項式の数

$$\lambda = \phi(2^n - 1)/n \quad (\phi(-): \text{Euler の関数})$$

となり¹⁾、 n が小さくなるときは N も λ も小さくなる。このような点を解決する方法として、シフトレジスタと非線形フィードバック回路を用いた 2 値ランダム系列発生法が提案されている²⁾⁻⁴⁾。しかし、これらの系列は、系列の性質が理論的に明らかでない²⁾、自己相関関数のサイドローブが M 系列の自己相関関数より大きい^{3), 4)}、などの欠点を有している。

これに対して、低次 M 系列を乱数を用いてランダムにサンプリングする方法は、簡単な方法で不規則性のよい 2 値ランダム系列を発生できると考えられる⁵⁾。そこで、本研究では M 系列をランダムにサンプリング

† 第 5 回計測自動制御学会九州支部学術講演会で発表 (昭 61・12)。

* 熊本大学工学部 熊本市黒髪 2-39-1

** 日本電気(株) 府中市日新町 1-10

* Faculty of Engineering, Kumamoto University, Kumamoto

** Nippon Electric Company, Fuchu

(Received April 30, 1987)

(Revised July 6, 1987)

する方法によって得られる2値ランダム系列の相関関数について述べる。

2. M系列のランダムサンプリング

まず、M系列を一定の間隔でサンプリングした場合について述べる。もとのM系列を $\{a_i\}$ とし、

$$\{a_i\} = a_0, a_1, \dots, a_{N-1}$$

$$a_i = 1 \text{ または } 0$$

と表わす。このとき $\{a_i\}$ を k 個ごとにサンプリングして得られる系列を $\{a_{ki}\}$ とすると、 $\{a_{ki}\}$ は次式のように表わされる。

$$\{a_{ki}\} = a_0, a_k, \dots, a_{k(N-1)}$$

上式において添字は mod N で考える。このとき、サンプリング間隔 k を N と互いに素にとると、 $\{a_{ki}\}$ は $\{a_i\}$ と同じ次数のM系列となる⁵⁾。特に、 $k=2^j$ (j : 正の整数) とした場合には、 $\{a_{ki}\}$ は $\{a_i\}$ と同じ特性多項式により発生したM系列となる⁵⁾。

これに対して、ランダムサンプリングではまず、M系列を連続して k 個 (以下、 k タップルと呼ぶ) 発生する。この場合、 k タップルを a_{ki} とおくと、 a_{ki} は(1)式のようになる (T は転置を表わす)。

$$a_{ki} = (a_{ki}, a_{ki+1}, \dots, a_{ki+k-1})^T \quad (1)$$

このとき、一様乱数 X_i ($i=0, 1, 2, \dots; 0 \leq X_i < 1$) を用いて a_{ki} の $[(k \cdot X_i) + 1]$ 番目のものを選ぶというのが本研究で述べるランダムサンプリングである。ここで、 $[-]$ はガウスの記号である。この方法によって得られる系列 $\{r_i\}$ は(1)式を用いて

$$\{r_i\} = a_{[k \cdot X_0]}, a_{[k \cdot X_1]}, \dots, a_{[k \cdot X_{N-1}]}, \dots$$

と表わすことができる。

3. ランダムサンプルされた系列の自己相関関数

2値ランダム系列を変調用符号などに用いる場合、系列の自己相関関数はデルタ関数に近いことが望ましい。そこで、本章では前章で述べたランダムサンプリングによって得られる系列 $\{r_i\}$ の自己相関関数について調べる。まず、Fig. 1(a)にもとのM系列 $\{a_i\}$ の自己相関関数 $\phi_{aa}(\tau)$ を示し、Fig. 1(b)に $\{a_i\}$ をランダムサンプリングして得られた系列 $\{r_i\}$ の自己相関関数 $\phi_{rr}(\tau)$ を示す。ここで、用いた特性多項式 $f(x)$ 、タップルの長さ k はそれぞれ、

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

$$k=5$$

である。ランダムサンプリングに用いる一様乱数としては、筆者らが作成した高次M系列を用いた乱数パッケージ⁶⁾を使用した。

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

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

Fig. 1 Autocorrelation function of original M-sequence $\{a_i\}$ and randomly sampled sequence $\{r_i\}$ where characteristic polynomial is $f(x) = x^7 + x^3 + 1$

また、自己相関関数を求める際には、0, 1 からなる系列 $\{a_i\}$, $\{r_i\}$ を次式のように ± 1 の2値からなる系列 $\{a'_i\}$, $\{r'_i\}$ に変換し、

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

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

$\{a_i\}$, $\{r_i\}$ を用いて、 $\phi_{aa}(\tau)$, $\phi_{rr}(\tau)$ を次式のように定義した⁹⁾。

$$\phi_{aa}(\tau) = \frac{1}{N} \sum_{i=0}^{N-1} a'_i \cdot a'_{i+\tau} = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{a_i} \cdot (-1)^{a_{i+\tau}} \quad (2)$$

$$\phi_{rr}(\tau) = \frac{1}{N} \sum_{i=0}^{N-1} r'_i \cdot r'_{i+\tau} = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{r_i} \cdot (-1)^{r_{i+\tau}} \quad (3)$$

Fig. 1(a), (b)を比較すると、もとのM系列の自己相関関数は $\tau=N$ において完全な周期性を示すのに対し、系列 $\{r_i\}$ の自己相関関数には規則性がみられない。したがって、系列 $\{r_i\}$ のほうがより不規則性のよい2値系列であるといえる。

Fig. 1 より、もとのM系列 $\{a_i\}$ の自己相関関数は遅れ $\tau=N$ において鋭いピークを示すが、系列 $\{r_i\}$ の自己相関関数には大きなピークは見られないことがわかる。

つぎに、 $\{r_i\}$ の自己相関関数の特徴をよりわかりやすくするため異なる乱数列を用いてランダムサンプ

リングを行い、得られた系列の自己相関関数を(3)式にしたがって求め、その集合平均を求めた。Fig. 2は特性多項式、タプル長を Fig. 1(b)と同じものとし、得られた系列 $\{r_i\}$ の自己相関関数 200 個の平均をとったものである。この図より、 $\tau=0$ 以外にもいくつかのピークが見られることがわかる。同様に、Fig. 3 は特性多項式を Fig. 2 の例と同じとし、タプル長を $k=4$ とした場合に得られる系列の自己相関関数 200 個の平均であり、Fig. 4 はタプル長を Fig. 2 と同じとし、特性多項式を

$$f(x)=x^7+x^5+x^3+x+1$$

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

Fig. 3 Ensemble averaged autocorrelation function of randomly sampled sequence $\{r_i\}$ where characteristic polynomial is $f(x)=x^7+x^3+1$ and tuple length is 4

Fig. 4 Ensemble averaged autocorrelation function of randomly sampled sequence $\{r_i\}$ where characteristic polynomial is $f(x)=x^7+x^5+x^3+x+1$ and tuple length is 5

としたときに得られる系列の自己相関関数 200 個の平均である。これらの図より、自己相関関数のピーク的位置は、

$$\tau = \frac{j \cdot N}{k} \quad (j: \text{正の整数})$$

であり、ピーク値はタプル長が同じであれば特性多項式によらず、ほぼ一定であることがわかる。

つぎに、系列 $\{r_i\}$ の自己相関関数の期待値 $E[\phi_{rr}(\tau)]$ の理論値を求める。まず、 $E[\phi_{rr}(\tau)]$ は(3)式より、次式のように表わされる。式中において $\oplus$ は排他的論理和を表わす。

$$\begin{aligned} E[\phi_{rr}(\tau)] &= E\left[\frac{1}{N} \sum_{i=0}^{N-1} (-1)^{r_i} \cdot (-1)^{r_{i+\tau}}\right] \\ &= E\left[\frac{1}{N} \sum_{i=0}^{N-1} (-1)^{r_i \oplus r_{i+\tau}}\right] \\ &= \frac{1}{N} \sum_{i=0}^{N-1} E[(-1)^{r_i \oplus r_{i+\tau}}] \end{aligned} \quad (4)$$

ここで、ランダムサンプリングに用いる乱数 X_i は区間 $[0, 1)$ において一様分布するため、

$$Pr[k \cdot X_i = j] = 1/k \quad (0 \leq j \leq k-1)$$

となる。上式より r_i が a_{ki} の各要素をとる確率は $1/k$ となり、

$$Pr\{r_i = a_{ki+j}\} = 1/k \quad (0 \leq j \leq k-1) \quad (5)$$

が得られ、 $(-1)^{r_i}$ の期待値 $E[(-1)^{r_i}]$ は(1)、(5)式を用いて次式のように表わされる。

$$E[(-1)^{r_i}] = \frac{1}{k} \sum_{j=0}^{k-1} (-1)^{a_{ki+j}} \quad (i=0, 1, 2, \dots) \quad (6)$$

また、乱数列 $\{X_i\}$ の各要素は互いに独立であるため、 $r_i \oplus r_{i+\tau} = a_{ki+j} \oplus a_{k(i+\tau)+l}$ ($0 \leq j, l \leq k-1$) となる確率は(5)式より、

$$\begin{aligned} Pr\{r_i \oplus r_{i+\tau} = a_{ki+j} \oplus a_{k(i+\tau)+l}\} \\ = Pr\{r_i = a_{ki+j}\} \cdot Pr\{r_{i+\tau} = a_{k(i+\tau)+l}\} \\ = 1/k^2 \end{aligned}$$

となり、次式が成り立つ。

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

上式を(4)式に代入して、

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

が得られる。

ここで、 k と N を互いに素にとると、前述のように系列 $\{a_{ki}\}$ は $\{a_i\}$ と同じ次数のM系列となる。そこで、系列 $\{a_{ki}\}$ を改めて $\{a_{ki}\} = \{b_i\}$ とおき、 d を $k \cdot d \equiv 1 \pmod{N}$ を満足する最小の正の整数とすると、

$$a_{ki+j} = a_{ki+jkd} = a_{k(i+jd)} = b_{i+jd}$$

となる⁷⁾。上式を(7)式に代入すると、

$$E[\phi_{rr}(\tau)] = \frac{1}{Nk^2} \sum_{i=0}^{N-1} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} (-1)^{b_{i+jd} \oplus b_{i+\tau+ld}} \quad (8)$$

が得られる。ここで、 $\{b_i\}$ の自己相関関数 $\phi_{bb}(\tau)$ を(2)式と同様に次式のように定義する⁹⁾。

$$\phi_{bb}(\tau) = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{b_i \oplus b_{i+\tau}}$$

上式を(8)式に代入して

$$\begin{aligned} E[\phi_{rr}(\tau)] &= \frac{1}{k^2} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{b_{i+jd} \oplus b_{i+\tau+ld}} \\ &= \frac{1}{k^2} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} \phi_{bb}(\tau + (l-j)d) \end{aligned} \quad (9)$$

が得られる。このとき、 $\{b_i\}$ はM系列であるため、

$$\phi_{bb}(\tau) = \begin{cases} 1 & (\tau = 0 \pmod{N}) \\ -1/N & (\tau \neq 0 \pmod{N}) \end{cases} \quad (10)$$

が成り立つ。(9)式をもとに、遅れ $\tau > 0$ の場合について $E[\phi_{rr}(\tau)]$ を求めると、以下ようになる。なお、 τ は $\text{mod } N$ で考える。

i) $\tau = s \cdot d$ ($s=0, 1, 2, \dots, k-1$) の場合

(9)式に $\tau = s \cdot d$ を代入すると、

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

となる。ここで、 $k \cdot d = 1 \pmod{N}$ より、 d と N は互いに素である。したがって、 $(s+l-j)d = 0 \pmod{N}$ となるのは、 $s+l-j=0$ のときに限られる。ここで、 $0 \leq j, l \leq k-1$ より $s+l-j=0$ となるのは $(k-s)$ 通り、 $s+l-j \neq 0$ となるのは、 (k^2-k+s) 通りである。よって(10)式を用いると、

$$\begin{aligned} E[\phi_{rr}(s \cdot d)] &= \frac{1}{k^2} \left\{ (k-s) - \frac{1}{N} (k^2 - k + s) \right\} \\ &= \frac{(N+1) \cdot (k-s) - k^2}{Nk^2} \end{aligned} \quad (11)$$

となる。

ii) $\tau = N - s \cdot d$ ($s=0, 1, 2, \dots, k-1$) の場合

i) の場合と同様に(10)式に τ を代入すると、

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

となる。ここで、 d と N は互いに素であるため、 $N - (l-j-s)d = 0 \pmod{N}$ となるのは、 $l-j-s=0$ のときである。また、 $0 \leq j, l \leq k-1$ より、 $l-j-s=0$ となるのは、 $(k-s)$ 通り、 $l-j-s \neq 0$ となるのが $(k^2 - k + s)$ 通りであるため、i) の場合と同様に、

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

が得られる。

iii) $\tau \neq s \cdot d$, $N - s \cdot d$ ($s=0, 1, 2, \dots, k-1$) の場合
このときは $0 \leq j, l \leq k-1$ のすべてについて $\tau + (l-j)d \neq 0$ となるため、(10)式より、

$$E[\phi_{rr}(\tau)] = \frac{1}{k^2} \cdot \left(-\frac{1}{N} \cdot k^2 \right) = -\frac{1}{N} \quad (13)$$

となる。

以上の結果より、系列 $\{r_i\}$ の自己相関関数の期待値はM系列の周期 N とタプル長 k で表わされ、特性多項式によらないことが示された。また、 $E[\phi_{rr}(\tau)]$ が最大値をとるのは、(11)、(12)式において $s=0$ とした $\tau = j \cdot N$ (j : 正の整数) のときであり、その値は

$$E[\phi_{rr}(j \cdot N)] = \frac{N - k + 1}{Nk} \quad (14)$$

である。上式において、次数 n を十分大きくとると $N \gg k$ となるため、

$$E[\phi_{rr}(j \cdot N)] \approx 1/k$$

となり、タプル長 k を長くとるほど、 $E[\phi_{rr}(j \cdot N)]$ の値を小さくすることができる。

実際に $\{r_i\}$ を発生して得られた自己相関関数の平均値を求め、上記のように求めた理論値と比較した結果を Fig. 5 に示す。この図はタプル長 k を $k=4, 8, 16$ とし、もとのM系列の次数 n を $n=5 \sim 12$ まで変えた場合の遅れ $\tau = N$ における自己相関関数200個の平均値である。この図より、実測値が(14)式の理論値とよく一致していることがわかる。平均回数を更に増せば両者の一致は更によくとも思われる。

つぎに、 $\phi_{rr}(\tau)$ のピーク値の分散について考える。前述のように、 $E[\phi_{rr}(\tau)]$ の値が最大となるのは(14)式のように $\tau = j \cdot N$ (j : 正の整数) の場合である。そこで、 $\phi_{rr}(N)$ の分散 σ^2 を求める。まず、(3)、(14)式より σ^2 は次式のようになる。

$$\sigma^2 = E[(\phi_{rr}(N))^2] - (E[\phi_{rr}(N)])^2$$

Fig. 5 Calculated and theoretical mean values of autocorrelation functions of randomly sampled sequences $\{r_i\}$

$$\begin{aligned}
 &= E\left[\frac{1}{N^2}\left(\sum_{i=0}^{N-1} (-1)^{r_i \oplus r_{i+N}}\right)^2\right] - \frac{(N-k+1)^2}{N^2 k^2} \\
 &= \frac{1}{N^2} E\left[\sum_{i=0}^{N-1} (-1)^{r_i \oplus r_{i+N}} \cdot \sum_{j=0}^{N-1} (-1)^{r_j \oplus r_{j+N}}\right] \\
 &\quad - \frac{(N-k+1)^2}{N^2 k^2} \quad (15)
 \end{aligned}$$

ここで、 $i=j$ ($0 \leq i, j \leq N-1$) のとき、 $r_i = r_j$, $r_{i+N} = r_{j+N}$ となるため、

$$(-1)^{r_i \oplus r_{i+N}} \cdot (-1)^{r_j \oplus r_{j+N}} = 1 \quad (16)$$

が成り立つ。また、 $i \neq j$ の場合は乱数列 $\{X_i\}$ の各要素は互いに独立であるため、

$$\begin{aligned}
 &E[(-1)^{r_i \oplus r_{i+N}}] \cdot E[(-1)^{r_j \oplus r_{j+N}}] \\
 &= E[(-1)^{r_i \oplus r_{i+N}}] \cdot E[(-1)^{r_j \oplus r_{j+N}}] \quad (17)
 \end{aligned}$$

が成り立つ。(16), (17)式を(15)式に代入すると、

$$\begin{aligned}
 \sigma^2 &= \frac{1}{N^2} \left\{ N + \sum_{i=0}^{N-1} E[(-1)^{r_i \oplus r_{i+N}}] \right. \\
 &\quad \cdot \sum_{j=0}^{N-1} E[(-1)^{r_j \oplus r_{j+N}}] \\
 &\quad \left. - \sum_{i=0}^{N-1} (E[(-1)^{r_i \oplus r_{i+N}}])^2 \right\} - \frac{(N-k+1)^2}{N^2 k^2} \quad (18)
 \end{aligned}$$

が得られる。ここで、(4), (14)式より、

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

となるため、(18)式は

$$\begin{aligned}
 \sigma^2 &= \frac{1}{N} - \frac{1}{N^2} \sum_{i=0}^{N-1} (E[(-1)^{r_i \oplus r_{i+N}}])^2 \\
 &= \frac{1}{N} - \frac{1}{N^2 k^4} \sum_{i=0}^{N-1} \left(\sum_{j=0}^{k-1} \sum_{l=0}^{k-1} (-1)^{a_{ki+j} \oplus a_{ki+l}} \right)^2
 \end{aligned}$$

となる。ここで a_{ki} 中の1の個数を t_i とすると、 $a_{ki+j} = a_{ki+l}$ となる場合が $t_i^2 - (k-t_i)^2$ 通り、 $a_{ki+j} \neq a_{ki+l}$ となる場合が $2t_i \cdot (k-t_i)$ 通りである。したがって、

$$\begin{aligned}
 \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} (-1)^{a_{ki+j} \oplus a_{ki+l}} &= t_i^2 - (k-t_i)^2 - 2t_i \cdot (k-t_i) \\
 &= (k-2t_i)^2
 \end{aligned}$$

となり、

$$\sigma^2 = \frac{1}{N} - \frac{1}{N^2 k^4} \sum_{i=0}^{N-1} (k-2t_i)^4 \quad (19)$$

が得られる。実際に、系列 $\{r_i\}$ を発生し、得られた自己相関関数の遅れ $\tau = N$ における分散を求めたところ、実測値は(19)式の理論値とよく一致した。

タプル長 k がM系列の周期と互いに素でない場合は $\{a_{ki}\}$ がM系列ではなくなり、(10)式が成り立たなくなる。このため、 $\{r_i\}$ の自己相関関数の期待値は $\{a_{ki}\}$ の自己相関関数を求めなければ得られない。例を Fig. 6 に示す。ここで、用いた特性多項式 $f(x)$

Fig. 6 Ensemble averaged autocorrelation function of randomly sampled sequence $\{r_i\}$ where characteristic polynomial is $f(x) = x^6 + x + 1$ and tuple length is 3

およびタプル長 k それぞれつぎのとおりである。

$$\begin{aligned}
 f(x) &= x^6 + x + 1 \\
 k &= 3
 \end{aligned}$$

Fig. 2~Fig. 4 では、系列 $\{r_i\}$ の自己相関関数の平均値はピーク値以外ではほぼ一定値であるのに対し、Fig. 6 の例ではさまざまな値を示し、(13)式が成り立っていないことがわかる。

4. ランダムサンプルされた系列同士の相互相関関数

2値ランダム系列をスペクトラム拡散通信の変調用符号などに用いる際には、系列同士の相互相関関数の値は小さくなければならない。そこで、ランダムサンプリングによって得られた系列同士の相互相関関数を求める。

まず、もとのM系列の次数 n およびタプル長 k を同じものとし、異なる一様乱数を用いてランダムサンプリングを行い得られた二つの系列を $\{r_i\}$, $\{p_i\}$ とする。このとき、 $\{r_i\}$ と $\{p_i\}$ の相互相関関数を次式のように定義する。

$$\phi_{rp}(\tau) = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{r_i \oplus p_{i+\tau}}$$

ここで k ともとのM系列の周期 N を互いに素にとると、 $\{r_i\}$, $\{p_i\}$ 発生に用いたM系列を k 個ごとにサンプルして得られる系列（これらの系列も次数 n のM系列となる）をそれぞれ、 $\{a_i\}$, $\{b_i\}$ とし、 $\{a_i\}$ と $\{b_i\}$ の相互相関関数 $\phi_{ab}(\tau)$ を

$$\phi_{ab}(\tau) = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{a_i \oplus b_{i+\tau}} \quad (20)$$

とする。このとき、 $\phi_{rp}(\tau)$ の期待値は(6)式と(20)式を用いると、

$$\begin{aligned}
 E[\phi_{rp}(\tau)] &= E\left[\frac{1}{N} \sum_{i=0}^{N-1} (-1)^{r_i \oplus p_{i+\tau}}\right] \\
 &= \frac{1}{N k^2} \sum_{i=0}^{N-1} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} (-1)^{a_{i+j} \oplus a_{i+\tau+l}}
 \end{aligned}$$

$$= \frac{1}{k^2} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} \phi_{ab}(\tau + (l-j)d) \quad (21)$$

となる. 上式より, $E[\phi_{ab}(\tau)]$ の最大値 $\phi_{\max}$ は以下のようなになる.

i) $\{a_i\} = \{b_i\}$ のとき, (14)式より

$$\phi_{\max} = \frac{N-k+1}{Nk} \quad (22)$$

ii) $\{a_i\} \neq \{b_i\}$ のとき,

$$\phi_{\max} < \max |\phi_{ab}(\tau)|$$

Table 1 Maximum absolute values of mean cross-correlation functions between randomly sampled sequences $\{r_i\}$ and $\{p_i\}$ where tuple length is 4.

The characteristic polynomials are

$$f_1(x) = x^5 + x^2 + 1,$$

$$f_2(x) = x^5 + x^4 + x^3 + x^2 + 1,$$

$$f_3(x) = x^5 + x^4 + x^3 + x + 1,$$

$$f_4(x) = x^5 + x^3 + x^2 + x + 1,$$

$$f_5(x) = x^5 + x^4 + x^3 + x + 1,$$

$$f_6(x) = x^5 + x^2 + 1.$$

$f(x)$ is the characteristic polynomial of M-sequence used for generating $\{r_i\}$.

$g(x)$ is the characteristic polynomial of M-sequence used for generating $\{p_i\}$

$f(x) \backslash g(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
$f_1(x)$	0.215	0.095	0.140	0.157	0.176	0.137
$f_2(x)$	0.125	0.234	0.168	0.122	0.110	0.168
$f_3(x)$	0.132	0.175	0.221	0.124	0.135	0.172
$f_4(x)$	0.163	0.119	0.125	0.205	0.168	0.126
$f_5(x)$	0.188	0.128	0.128	0.166	0.222	0.138
$f_6(x)$	0.129	0.172	0.170	0.121	0.125	0.217

Table 2 Maximum absolute values of mean cross-correlation functions between randomly sampled sequences $\{r_i\}$ and $\{p_i\}$ where tuple length is 8.

The characteristic polynomials are the same as those at Table 1.

$f(x)$ is the characteristic polynomial of M-sequence used for generating $\{r_i\}$.

$g(x)$ is the characteristic polynomial of M-sequence used for generating $\{p_i\}$

$f(x) \backslash g(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
$f_1(x)$	0.104	0.083	0.093	0.080	0.077	0.078
$f_2(x)$	0.097	0.111	0.091	0.086	0.071	0.078
$f_3(x)$	0.087	0.088	0.104	0.082	0.089	0.082
$f_4(x)$	0.084	0.084	0.089	0.097	0.092	0.097
$f_5(x)$	0.078	0.077	0.088	0.083	0.085	0.072
$f_6(x)$	0.075	0.098	0.093	0.093	0.086	0.091

ここで $\{a_i\} = \{b_i\}$ の場合, (22)式より, タップル長 k を大きくとるほど, $\phi_{\max}$ の値は小さくなる. また, $\{a_i\} \neq \{b_i\}$ の場合も k が大きくなると, (21)式の右辺は $\phi_{ab}(\tau)$ の平均値に近づくため, $\phi_{\max}$ の値は小さくなり, より特性のよい 2 値ランダム系列を発生できると考えられる.

実際に, 5 次の M 系列をもとに $\{r_i\}$, $\{p_i\}$ を発生し, 相互相関関数の集合平均をとり, その絶対値の最大値を求めた結果を Table 1, 2 に示す. ここで, タップル長 k は, Table 1 が $k=4$, Table 2 が $k=8$ であり, 平均の回数はそれぞれ 200 回である. これらの結果より, タップル長を大きくとるほど, 相互相関関数の最大値は小さくなっていることがわかり, 上述の推測が妥当であるといえる.

5. あとがき

本研究では, 2 値ランダム系列の簡単な発生法として, 一様乱数を用いて低次 M 系列をランダムにサンプリングするという方法を提案した. そして, この方法により得られる 2 値ランダム系列の自己相関関数の期待値を理論的に求め, その値が用いた M 系列の周期とタップル長によって決定されることを示した.

さらに, この方法によって得られる系列同士の相互相関関数を求め, もとの M 系列が異なる場合, 相互相関関数の期待値の最大値がもとの M 系列の相互相関関数の最大値よりも小さくなることを示した. また, 実際に発生した系列の相互相関関数の集合平均を求め, タップル長を大きくとるほど, それらの最大値が小さくなることを示した.

参考文献

- 1) S. W. Golomb: Shift Register Sequence, Holden-Day (1967)
- 2) 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)
- 3) S. M. Jennings: Autocorrelation Function of the Multiplexed Sequence, IEE Proc. F, Commun. Radar & Signal Process., **131-2**, 169/172 (1984)
- 4) J. D. Olsen, R. A. Sholtz and L. R. Welch: Bent Function Sequence, IEEE Trans. Information Theory, **IT-28-6**, 856/864 (1982)
- 5) 柏木: M 系列再発見, 計測と制御, **20-2**, 236/245 (1981)
- 6) 原田, 柏木: M 系列を用いる乱数発生法, 計測自動制御学会論文集, **23-8**, 806/811 (1987)
- 7) 柏木: M 系列による TLP 乱数の二, 三の性質, 計測自動制御学会論文集, **18-8**, 828/832 (1982)
- 8) 原田, 柏木, 小栗: M 系列をランダムにサンプリングした系列の相関関数, 第 5 回計測自動制御学会九州支部學術講演会予稿集, 59/60 (1986)
- 9) F. J. McWilliams and N. J. A. Sloane: Pseudo-Random Sequences and Arrays, Proc. IEEE, **64-12**, 1715/1729 (1976)