M 系列をランダムにサンプルした系列の性質†

原 田 博 之*・柏 木 潤*・本 多 敏*・小 栗 一 男**

On Some Properties of Randomly Sampled M-Sequence

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

This paper describes some properties of randomly sampled M-sequence, and compares those properties for two methods of sampling. The first method, called method I, is to sample $(\lfloor k \cdot w_i \rfloor + 1)$ 'st bit from a k -tuple of an M-sequence, where w_i is a random number having any distribution function between 0 and 1. The second method, called method II, is to sample $(\lfloor k \cdot X_i \rfloor + 1)$ 'st bit from a $(\lfloor k \cdot X_i \rfloor + 1)$ -tuple of M-sequence, where X_i is a uniform random number between 0 and 1.

It is shown that the maximum value of the ensemble averaged autocorrelation function in case of method I becomes minimum when w_i is a uniform random number. It is also shown that the maximum value of the ensemble averaged autocorrelation function of randomly sampled sequence generated by method II is smaller than that of the sequence generated by method I.

From these results, we see that method II is better than method I in order to get a binary random sequence having good random properties.

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

1. ま え が き

2 値ランダム系列はスペクトラム拡散通信の変調用符号等にさかんに用いられている。M 系列信号はこの 2 値ランダム系列としてよく用いられる系列の一つであるが、次数が低い場合にはその周期はきわめて短いものになる、系列のうち長さ $2n$ (n : M 系列の次数)

の部分列がわかれば系列の残りの部分はすべて決定されるという単純な構造であるなどの欠点がある。M 系列のもつこれらの欠点を改善し、低次 M 系列を用いてより複雑な構造をもつ 2 値ランダム系列の発生法として、筆者らは先に低次 M 系列を一定のタプル長発生し、一様乱数を用いてその中から一つの要素を選ぶという方法（以下、方法 I と呼ぶ）を提案し、この方法によって得られる系列の自己相関関数の期待値を求めた^{1), 2), 4)}。そして、方法 I により得られる 2 値系列の自己相関関数の期待値が遅れ $\tau = j \cdot N$ (j : 正の整数, N : もとの M 系列の周期) において最大値をとることを示した。

なぜ、一様乱数を用いて M 系列をランダムにサンプルするかという点についてはつぎのように考える。もし、理想的な一様乱数が存在するならば、特性のよい 2 値ランダム系列の発生は容易である。しかし、実際によく用いられる乱数発生法である Lehmer 型合同法により発生した乱数は多次元空間において一様な分布を示さない³⁾。このため合同法乱数のみを用いたのでは特性のよい 2 値ランダム系列は得られない。これに対して、筆者らの提案した方法は一様乱数の不規則性にある程度問題がある場合でも、低次 M 系列と組み合わせることにより、特性のよい 2 値ランダム系列が発生できると考えられる。

本研究ではまず、この方法により獲られる 2 値ランダム系列の自己相関関数の期待値の最大値を最小にするための条件を示す。つぎに、より自己相関関数の期待値の最大値が小さく不規則性の良い 2 値ランダム系列の発生法として、タプル長をランダムにとる方法を提案し、この方法によって得られる系列の自己相関関数の期待値の最大値を求める。

2. 方法 I により得られる系列の自己相関関数

文献 1), 2) で提案した 2 値ランダム系列発生法(方

† 第 26 回計測自動制御学会学術講演会で発表(昭 62・7)

* 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 Co., Fuchu

(Received June 13, 1987)

(Revised April 14, 1988)

法 I) は, n 次の M 系列 $\{a_i\}$ を連続して k 個 (以下, k タップルと呼ぶ) 発生し, 区間 $[0, 1)$ において一様分布する乱数 $X_i (i=0, 1, 2, \dots)$ を用いて, k タップルの要素のうちの $(\lfloor k \cdot X_i \rfloor + 1)$ 番目の要素を選ぶ ($\lfloor \cdot \rfloor$ はガウスの記号) というものである. このとき, 方法 I) により得られる系列を $\{r_i\}$ とすると, タップル長 k が M 系列 $\{a_i\}$ の周期 $N=2^n-1$ と互いに素であり, 乱数列 $\{X_i\}$ の各要素が互いに独立であるならば (注 1), $\{r_i\}$ の自己相関関数の期待値 $E[\phi_{rr}(\tau)]$ は (1) 式のようなになる^{2), 4)}. ここで, d は (2) 式を満足する最小の正の整数である.

$$E[\phi_{rr}(\tau)] = \begin{cases} \frac{(N+1) \cdot (k-s) - k^2}{Nk^2} & (\tau = s \cdot d, N-s \cdot d) \\ -\frac{1}{N} & (\tau \neq s \cdot d, N-s \cdot d) \end{cases} \quad (1)$$

$$(0 \leq s \leq k-1)$$

$$k \cdot d \equiv 1 \pmod{N} \quad (2)$$

なお, 本論文では, $0, 1$ からなる任意の 2 値系列 $\{m_i\}$ の自己相関関数 $\phi_{mm}(\tau)$ は次式のように定義する.

$$\phi_{mm}(\tau) = \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{m_i} \cdot (-1)^{m_{i+\tau}}$$

また, 添字はすべて $\text{mod } N$ で考えるものとする.

ここで, 方法 I) でランダムサンプリングに用いる乱数として, 区間 $[0, 1)$ において任意の分布をもつ乱数列 $\{w_i\} (i=0, 1, 2, \dots)$ を用いて, k タップルの $(\lfloor k \cdot w_i \rfloor + 1)$ 番目のものを選ぶ場合について考える. このとき, 得られる 2 値系列を $\{v_i\}$ とすると,

$$\{v_i\} = a_{\lfloor k \cdot w_0 \rfloor}, a_{\lfloor k \cdot w_1 \rfloor}, \dots, a_{\lfloor k \cdot w_{k-1} \rfloor}, \dots$$

と表わされる. また,

$$\Pr\left\{\frac{j}{k} \leq w_i < \frac{j+1}{k}\right\} = p_j \quad (0 \leq j \leq k-1)$$

$$\sum_{j=0}^{k-1} p_j = 1$$

とすると, $(-1)^{v_i}$ の期待値は

$$E[(-1)^{v_i}] = \sum_{j=0}^{k-1} p_j \cdot (-1)^{a_{ki+j}} \quad (3)$$

と表わすことができる.

つぎに, $\{v_i\}$ の自己相関関数の期待値 $E[\phi_{vv}(\tau)]$ は w_i と $w_{i+\tau}$ が互いに独立ならば, (3) 式を用いて次式のように表わされる.

$$E[\phi_{vv}(\tau)] = \frac{1}{N} \sum_{i=0}^{N-1} E[(-1)^{v_i} \cdot (-1)^{v_{i+\tau}}]$$

(注 1) 各要素が互いに独立であるような理想的な一様乱数の発生は困難であるが, 本研究では理論的解析を容易にするため, このような乱数列を仮定した.

$$= \frac{1}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} p_j \cdot p_l \cdot (-1)^{a_{ki+j}} \cdot (-1)^{a_{k(i+\tau)+l}} \quad (4)$$

ここで k と N が互いに素な場合, $\{a_{ki}\}$ は $\{a_i\}$ と同じ次数の M 系列となるので, $\{a_{ki}\} = \{b_i\}$ とおくと (2) 式より

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

となる³⁾. これを (4) 式に代入すると,

$$E[\phi_{vv}(\tau)] = \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} p_j \cdot p_l \cdot \frac{1}{N} \sum_{i=0}^{N-1} (-1)^{b_{i+jd}} \cdot (-1)^{b_{i+\tau+ld}} \\ = \sum_{j=0}^{k-1} \sum_{l=0}^{k-1} p_j \cdot p_l \cdot \phi_{bb}(\tau + (l-j)d) \quad (5)$$

が成り立つ. (5) 式をもとに, 遅れ $\tau > 0$ の場合について $E[\phi_{vv}(\tau)]$ を求めると以下のようなになる. ここで, 遅れは $\text{mod } N$ で考える.

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

$\tau = s \cdot d$ を (6) 式に代入して,

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

が得られる. (2) 式より, d と N は互いに素であるため, $l = j-s$, $s \leq j \leq k-1$ のときに $(s+l-j)d = 0$ となり, $\{b_i\}$ が M 系列であるため, $\phi_{bb}((s+l-j)d) = 1$ となる. また, それ以外の場合は, $\phi_{bb}((s+l-j)d) = -1/N$ となる. これらを上式に代入して, (6) 式が得られる.

$$E[\phi_{vv}(s \cdot d)] = \sum_{j=s}^{k-1} p_j \cdot p_{j-s} \\ - \frac{1}{N} \left\{ \sum_{j=s}^{k-1} p_j \left(\sum_{l=0}^{k-1} p_l - p_{j-s} \right) \right. \\ \left. + \sum_{j=0}^{s-1} p_j \cdot \sum_{l=0}^{k-1} p_l \right\} \\ = \sum_{j=s}^{k-1} p_j \cdot p_{j-s} - \frac{1}{N} \left\{ \sum_{j=s}^{k-1} p_j \cdot (1 - p_{j-s}) \right. \\ \left. + \sum_{j=0}^{s-1} p_j \right\} \quad (6)$$

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

(i) と同様に (5) 式に $\tau = N-s \cdot d$ を代入すると,

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

となる. ここで, d と N は互いに素であるため, $l = j+s$, $0 \leq j \leq k-s-1$ のときに $N-(l-j-s)d = 0 \pmod{N}$ となる. よって, (i) の場合と同様のやり方で, 次式が得られる.

$$E[\phi_{vv}(N-s \cdot d)] = \sum_{j=0}^{k-s-1} p_j \cdot p_{j+s}$$

$$\begin{aligned}
 & -\frac{1}{N} \left\{ \sum_{l=0}^{k-s-1} p_j \left(\sum_{l=0}^{k-1} p_l - p_{j+s} \right) \right. \\
 & \quad \left. + \sum_{j=k-s}^{k-1} p_j \cdot \sum_{l=0}^{k-1} p_l \right\} \\
 & = \sum_{j=0}^{k-s-1} p_j \cdot p_{j+s} \\
 & \quad - \frac{1}{N} \left\{ \sum_{j=0}^{k-s-1} p_j (1 - p_{j+s}) \right. \\
 & \quad \left. - \sum_{j=k-s}^{k-1} p_j \right\} \quad (7)
 \end{aligned}$$

(iii) $\tau \neq s \cdot d$, $N - s \cdot d$ の場合 ($0 \leq s \leq k-1$)

この場合, $0 \leq j, l \leq k-1$ のすべてにおいて $\tau + (l-j)d \neq 0 \pmod{N}$ となる。したがって, $E[\phi_{vv}(\tau)]$ は

$$E[\phi_{vv}(\tau)] = -\frac{1}{N}$$

となる。

実際に, 任意の乱数列を用い, 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求めた例を **Fig. 1(a)** に示す。ここで, もとの M 系列の特性多項式 $f(x)$ およびタプル長 k は,

$$\begin{aligned}
 f(x) &= x^7 + x^3 + 1 \\
 k &= 5
 \end{aligned} \quad (8)$$

(a) An example of autocorrelation function of $\{v_i\}$

(b) Ensemble averaged autocorrelation function of $\{v_i\}$ when averaging number is 200

Fig. 1 Ensemble averaged autocorrelation function of randomly sampled sequence $\{v_i\}$ generated by method I where the characteristic polynomial of original M-sequence is $f(x) = x^7 + x^3 + 1$ and tuple length is 5

であり, ランダムサンプリングに用いた乱数は平均値 μ , 標準偏差 σ がそれぞれ,

$$\mu = \frac{1}{2} \quad \sigma = \frac{1}{6}$$

である正規乱数である。また, **Fig. 1(b)** に上記の条件で異なる 200 個の乱数列を用いてランダムサンプリングを行い, 得られた自己相関関数の集合平均をとったものを示す。

つぎに, (6)式および(7)式において, $s=0$ としたときの遅れ $\tau=N$ における理論値と実測値を比較した結果を **Fig. 2** に示す。用いた乱数は **Fig. 1** の例と同じ平均値と標準偏差を有する正規乱数であり, もとの M 系列の次数 n およびタプル長 k は, $n=5 \sim 12$, $k=4, 8, 16$ である。また, 実測値は 100 個の自己相関関数の集合平均をとったものである。この図より, 理論値と実測値はよく一致しているといえる。

2 値ランダム系列を変調用符号などに用いる場合, その自己相関関数の最大値はできるだけ小さいことが望ましい。ここで, 方法 I により得られる系列の場合, $E[\phi_{vv}(\tau)]$ が遅れ $\tau > 0$ において最大値をとるのは, (6), (7)式において $s=0$ としたとき, すなわち, 遅れ $\tau = j \cdot N$ (j : 正の整数) のときである。このとき (6), (7)式に $s=0$ を代入して,

$$\begin{aligned}
 \max E[\phi_{vv}(\tau)] &= E[\phi_{vv}(j \cdot N)] \\
 &= \sum_{j=0}^{k-1} p_j^2 - \frac{1}{N} \sum_{j=0}^{k-1} p_j (1 - p_j) \\
 &= \left(1 + \frac{1}{N}\right) \sum_{j=0}^{k-1} p_j^2 - \frac{1}{N} \quad (9)
 \end{aligned}$$

となる。一方, $E[\phi_{rr}(\tau)]$ が $\tau > 0$ において最大値をとるのも, (1)式において, $s=0$ とした遅れ $\tau = j \cdot N$ のときであり, その値は,

Fig. 2 Calculated and theoretical maximum values of ensemble averaged autocorrelation functions of randomly sampled sequence $\{v_i\}$ generated by method I where averaging number is 100

$$\max E[\phi_{rr}(\tau)] = \frac{N-k+1}{Nk} \quad (10)$$

である。ここで、

$$\sum_{j=0}^{k-1} p_j^2 \leq \sum_{j=0}^{k-1} \frac{1}{k^2} = \frac{1}{k}$$

を(9)式に代入すると、次式が成り立つ。

$$\begin{aligned} \max E[\phi_{vv}(\tau)] &\geq \left(1 + \frac{1}{N}\right) \cdot \frac{1}{k} - \frac{1}{N} \\ &= \frac{N-k+1}{Nk} \\ &= \max [E\phi_{rr}(\tau)] \end{aligned}$$

上式より、方法Ⅰによりランダムサンプリングを行う場合、得られる系列の自己相関関数の期待値の最大値を最小にするためには、一様乱数を用いればよいといえる。

3. タップル長をランダムにとる方法 により得られる系列の自己相関関数

本章では、各要素が互いに独立であるような一様乱数列を用いた新たなランダムサンプリングの方法として、タップル長をランダムにとる方法（以下、方法Ⅱと呼ぶ）を提案し、この方法により得られる系列の性質について述べる。方法Ⅱの場合も方法Ⅰと同様にM系列をkタップル発生し、別に発生した一様乱数 $X_i (i=0, 1, 2, \dots)$ を用いてkタップルのうちの $(\lfloor k \cdot X_i \rfloor + 1)$ 番目の要素を選ぶが、つぎのkタップルを発生する際に、選んだ要素のつぎの要素から発生するという点が異なる。すなわち、方法ⅡはM系列を $(\lfloor k \cdot X_i \rfloor + 1)$ タップル発生し、その最後の要素を選ぶという方法である。このとき、方法Ⅱにより得られる系列を $\{q_i\}$ とし、

$$q_i = a_{j(i)}$$

とおくと、

$$\begin{aligned} j(i) &= j(i-1) + \lfloor k \cdot X_i \rfloor + 1 \\ &= j(i-2) + \lfloor k \cdot X_i \rfloor + \lfloor k \cdot X_{i-1} \rfloor + 2 \\ &\vdots \\ &= i + \sum_{l=0}^{i-1} \lfloor k \cdot X_l \rfloor \end{aligned}$$

となり、系列 $\{q_i\}$ は次式のように表わされる。

$$\{q_i\} = a_{\lfloor k \cdot X_0 \rfloor}, a_{1 + \lfloor k \cdot X_0 \rfloor + \lfloor k \cdot X_1 \rfloor}, \dots, a_{i + \sum_{l=0}^{i-1} \lfloor k \cdot X_l \rfloor}, \dots$$

ここで、 X_i は一様乱数であるため、

$$\Pr \{\lfloor k \cdot X_i \rfloor = l\} = \frac{1}{k} \quad (0 \leq l \leq k-1) \quad (11)$$

となる。このとき、乱数列 $\{X_i\}$ の各要素が互いに独立であるならば、次式が成り立つ。

$$\Pr \{j(0) = l_0\} = \frac{1}{k} \quad (0 \leq l_0 \leq k-1)$$

$$\Pr \{j(i) = j(i-1) + 1 + l_i\} = \frac{1}{k}$$

$$(0 \leq l_i \leq k-1, i=1, 2, \dots) \quad (12)$$

上式を用いると、 q_i の期待値 $E[q_i]$ は次式のように表わすことができる。

$$\begin{aligned} E[q_i] &= \frac{1}{k} \sum_{l_i=0}^{k-1} a_{j(i-1)+1+l_i} \\ &= \frac{1}{k} \sum_{l_i=0}^{k-1} \frac{1}{k} \sum_{l_{i-1}=0}^{k-1} a_{j(i-2)+2+l_i+l_{i-1}} \\ &= \frac{1}{k^{i+1}} \sum_{l_0=0}^{k-1} \sum_{l_1=0}^{k-1} \dots \sum_{l_{i-1}=0}^{k-1} a_{i+l_0+l_1+\dots+l_i} \quad (13) \end{aligned}$$

(13)式と(3)式を比較すると、方法Ⅰにより得られた系列はkタプルのいずれかしかとりえないのに対し、方法Ⅱでは、系列 $\{q_i\}$ の発生個数 i が大きくなると、

$$\Pr \{q_i = a_i\} \neq 0 \quad (0 \leq i \leq N-1)$$

となり、 q_i は系列 $\{a_i\}$ のすべての要素のいずれかをとり可能性がある。したがって、もとのM系列の次数およびタップル長 k が同じ場合、方法Ⅱのほうがより不規則性のよい2値系列を発生できると考えられる。

実際に、系列 $\{q_i\}$ の自己相関関数 $\phi_{qq}(\tau)$ を求めた例をFig. 3(a)に、異なる乱数列を用いて得られ

(a) An example of autocorrelation function of $\{q_i\}$

(b) Ensemble averaged autocorrelation function of $\{q_i\}$ when averaging number is 200

Fig. 3 Ensemble averaged autocorrelation function of randomly sampled sequence $\{q_i\}$ generated by method II where the characteristic polynomial of original M-sequence is $f(x) = x^7 + x^3 + 1$ and maximum tuple length is 5

た 200 個の $\phi_{qq}(\tau)$ の集合平均を Fig. 3(b) に示す。ここで、もとの M 系列の特性多項式およびタップ長は Fig. 1 と同じものである。これより、 $\phi_{qq}(\tau)$ の集合平均はある遅れ τ_m (Fig. 3 の例では $\tau_m=42$) の整数倍の遅れにおいてピークを示すが、その形は $E[\phi_{rr}(\tau)]$ の場合のような鋭いものではなく、ピーク値も小さいことがわかる。

つぎに、 $\phi_{qq}(\tau)$ の期待値 $E[\phi_{qq}(\tau)]$ が最大値をとる遅れ τ_m を求める。もとの M 系列 $\{a_i\}$ の一周期を用いて発生した $\{q_i\}$ の長さの平均を L_q とすると、 q_i と q_{i+L_q} は $\{a_i\}$ のほぼ同じ部分をサンプルして得られたものとなる。このため、遅れ L_q における $\{q_i\}$ の自己相関関数の値が大きくなり、 $\tau_m=L_q$ となると考えられる。このとき、 q_i を 1 個発生するのに必要な a_i の個数の平均を j_m とすると、 L_q は j_m を用いて

$$L_q = \frac{N}{j_m} \quad (14)$$

と表わされる。ここで、(11)式より

$$\begin{aligned} j_m &= E[j(i) - j(i-1)] = \sum_{l=0}^{k-1} (l+1) \cdot \Pr[k \cdot X_i = l] \\ &= \frac{k+1}{2} \end{aligned}$$

が成り立つ。上式を(14)式に代入して、

$$\tau_m = L_q = \frac{2N}{k+1} \quad (15)$$

が得られる。実際に $\{q_i\}$ を発生し、得られた自己相関関数の集合平均より求めた τ_m と(15)式の理論値との比較を行った結果を Fig. 4 に示す。Fig. 4 はもとの M 系列 $\{a_i\}$ の次数 n を $n=5, 6, 7$ とし、タップ長 k を $k=2 \sim 10$ としたとき得られる $\{q_i\}$ の自己相関関数 50 個の平均より τ_m を求めたものである。この図より、(15)式の理論値が τ_m の実測値とよく一致しているといえる。

Fig. 4 Calculated and theoretical delays where the ensemble averaged autocorrelation functions of randomly sampled sequence $\{q_i\}$ generated by method II shows maximum value. Averaging number is 50

系列 $\{q_i\}$ の自己相関関数の期待値の理論値は方法 I の場合のように簡単には求められない。しかし、その最大値、すなわち $E[\phi_{qq}(\tau_m)]$ は以下のように求めることができる。系列 $\{q_i\}$ の自己相関関数を求めるとき、 q_i と $q_{i+\tau}$ の値が一致する個数を A 、両者の値が異なる個数を D とすると、 $\phi_{qq}(\tau)$ は次式のように定義することができる⁵⁾。

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

ここで、上式の両辺の期待値をとると、

$$E[\phi_{qq}(\tau)] = \frac{E[A] - E[D]}{N} \quad (16)$$

となる。ここで、遅れ $\tau \neq \tau_m$ の場合については、もとの M 系列中の 0, 1 の個数はほぼ等しいため、 q_i と $q_{i+\tau}$ の値が一致する確率と両者の値が異なる確率はほぼ等しくなるため、 $E[A] \approx E[D]$ となり、

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

となる。ところが、遅れ $\tau = \tau_m$ の場合、前述のように q_i と $q_{i+\tau_m}$ はもとの M 系列 $\{a_i\}$ のほぼ同じ部分をサンプルして得られるため、両者が $\{a_i\}$ の同じ要素をとる場合がある。この場合 $j(i) = j(i + \tau_m)$ となり、 q_i と $q_{i+\tau_m}$ の値は一致する。一方、 $j(i) \neq j(i + \tau_m)$ の場合には、両者が一致する確率と異なる確率は等しくなる。したがって、 $E[A]$ および $E[D]$ は

$$\begin{aligned} E[A] &= \sum_{i=0}^{N-1} \Pr\{j(i) = j(i + \tau_m)\} \\ &\quad + \frac{1}{2} \sum_{i=0}^{N-1} \Pr\{j(i) \neq j(i + \tau_m)\} \\ E[D] &= \frac{1}{2} \sum_{i=0}^{N-1} \Pr\{j(i) \neq j(i + \tau_m)\} \end{aligned}$$

と表わされる。これらを(16)式に代入して、

$$E[\phi_{qq}(\tau_m)] = \frac{1}{N} \sum_{i=0}^{N-1} \Pr\{j(i) = j(i + \tau_m)\} \quad (17)$$

が得られる。

ここで、(17)式中の $\Pr\{j(i) = j(i + \tau_m)\}$ は以下のように求めることができる。

$$\begin{aligned} \Pr\{j(i) = j(i + \tau_m)\} &= \sum_{l=0}^{N-1} \Pr\{j(i) = l\} \cdot \\ &\quad \Pr\{j(i + \tau_m) = l\} \\ &= \sum_{l=0}^{N-1} (\Pr\{j(i) = l\})^2 \end{aligned}$$

また、上式の $\Pr\{j(i) = l\}$ ($0 \leq l \leq N-1$) は(12)式を用いて、

$$\begin{aligned} \Pr\{j(i) = l\} &= \frac{1}{k} \sum_{s=0}^{k-1} \Pr\{j(i-1) \\ &\quad = l - s - 1 \pmod{N}\} \end{aligned}$$

Fig. 5 Calculated and theoretical maximum values of ensemble averaged autocorrelation functions of randomly sampled sequences generated by method I and method II where the characteristic polynomial of the original M-Sequence is $f(x)=x^7+x^3+1$ and averaging number is 1,000

$$\Pr\{j(0)=l\} = \begin{cases} \frac{1}{k} & (0 \leq l \leq k-1) \\ 0 & (k \leq l \leq N-1) \end{cases}$$

より求められる。

実際に方法Ⅰと方法Ⅱにより系列 $\{r_i\}$ と $\{q_i\}$ を発生し、得られた自己相関関数 1,000 個の集合平均 $\phi_{rr}(\tau)$ および $\phi_{qq}(\tau)$ の $\tau > 0$ における最大値を求め、(10)式および(17)式の値と比較した結果を Fig. 5 に示す。ここで、もとの M 系列の特性多項式は(8)式を用い、タッフル長 k は $k=2 \sim 10$ とした。この図より方法Ⅱについては、特に k が大きいとき、(17)式の予測値が実測値とよく一致しており、上記の推論が妥当であり、(17)式を用いることにより $E[\phi_{qq}(\tau)]$ の最大値の評価ができると考えられる。また、方法Ⅰと方法Ⅱにより得られる系列の自己相関関数を比べた場合、もとの M 系列の特性多項式とタッフル長が等しいときは常に、

$$\max E[\phi_{qq}(\tau)] < \max E[\phi_{rr}(\tau)]$$

が成り立ち、方法Ⅱのほうがより不規則性のよい 2 値ランダム系列を発生できると考えられる。

4. あとがき

本論文では、低次 M 系列をランダムにサンプルす

る方法により得られる系列の性質について、以下のことを明らかにした。

まず、タッフル長を一定にとる方法(方法Ⅰ)において、区間 $[0, 1)$ で任意の分布をもつ乱数を用いてランダムサンプリングを行った場合について、得られる 2 値ランダム系列の自己相関関数の期待値の理論値を求めた。そして、その最大値を最小とするためには、一様乱数を用いてランダムサンプリングを行えばよいことを示した。

つぎに、より不規則性のよい 2 値ランダム系列の発生法としてタッフル長をランダムにとる方法(方法Ⅱ)を提案し、方法Ⅱにより得られる系列の自己相関関数の期待値が最大となる遅れ τ_m および、最大値の予測値を導いた。さらに、実際に同じ M 系列を用いて、方法Ⅰおよび方法Ⅱにより 2 値ランダム系列を発生し、得られた自己相関関数の集合平均の遅れ $\tau > 0$ における最大値を求めたところ、これらの実測値が予測値とよく一致しており、方法Ⅱにより得られた系列のほうが集合平均をとった自己相関関数の最大値が小さくなることが確認された。以上の結果より、低次 M 系列を用いて 2 値ランダム系列を発生する方法としては、タッフル長をランダムにとる方法がより優れていると考えられる。

参考文献

- 1) 原田, 柏木, 小栗: M 系列をランダムにサンプルした系列の相関関数, 第 5 回計測自動制御学会九州支部学術講演会予稿集, 59/60 (1986)
- 2) 原田, 柏木, 本多, 小栗: 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, 計測自動制御学会論文集, 23-11, 1145/1150 (1987)
- 3) 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)
- 4) H. Harada, H. Kashiwagi, S. Honda and K. Oguri: Binary Random Sequence Generation by Use of Random Sampling of M-Sequence, Proc. of '87 KACC, 832/835 (1987)
- 5) F.J. McWilliams and N.J.A. Sloane: Pseudo-Random Sequences and Arrays, Proc. IEEE, 64-12, 1715/1729 (1976)
- 6) G. Marsaglia: Random Numbers Fall Mainly in the Planes, Proc. Nat. Acad. Sci., 61, 26/28 (1968)