M 系列の部分的性質の類似性の評価†

原 田 博 之*・柏 木 潤*

Evaluation of Resemblance of Partial Properties of M-Sequence

Hiroshi HARADA* and Hiroshi KASHIWAGI*

This paper proposes a new concept "resemblance" for evaluating the partial resemblance between any two phases of an M-sequence. By use of this concept, we can evaluate the resemblance quantitatively.

The authors first show that the partial properties of M-sequence are influenced by runs of 0's or 1's in the initial n -tuple of M-sequence. Then a new concept called resemblance is proposed for evaluating the resemblance between any two n -tuples. The resemblance between the initial n -tuple at phase 0 and the n -tuple at several phases is calculated. The results show that the new concept "resemblance" is very effective for evaluating the resemblance between the partial properties of M-sequence.

Key Words: M-sequence, pseudo-random sequence, phase of M-sequence, partial properties of M-sequence

1. ま え が き

現在、計算機のライブラリプログラムとして用いられる擬似乱数発生法としては、Lehmer 型合同法が主である。しかし、この方法により発生した擬似乱数は、①多次元分布が一様でない¹⁾、②周期が計算機の語長により制限されるなどの欠点を有している。

一方、高次M系列を用いた擬似乱数発生法は合同法にみられる欠点をもたないため近年盛んに研究されており^{2)~4)}、最近では大型計算機内にハードウェアとして組みこまれているものもある。ただ、この方法により擬似乱数を発生する際、M系列の初期 n タップル (n : M系列の次数) として不適当なもの、たとえば特性M系列の初期 n タップルなどを選ぶと、発生した擬

似乱数の最初の部分はきわめて不規則性の悪いものとなる⁵⁾。またこの場合、初期値として用いた n タップルを位相原点としたとき、円分位相点 ($(\text{周期}+1)/2^i$ 位相点, i : 正の整数) の n タップルを用いて発生した擬似乱数も最初の部分が不規則性の悪いものになることが知られている⁵⁾。さらにM系列の特性多項式がある特定の形になる場合には、円分位相点だけでなく、 i/s 位相点 ($s=2^m+1$ または 7, $1 \leq i \leq s-1$) においても同様の性質を示すことが指摘されている⁶⁾。

このようなM系列の各位相点における類似性の評価方法として、これまでの研究では実際に各位相点よりM系列を発生してその部分的性質 (部分的自己相関関数、連の部分的自己相関関数など) の類似性をみるというものであった^{5)~7)}。しかし、この方法では各位相点の類似性を定量的に評価することはできない。また、実際にM系列を発生しなければ部分的性質を求められないという点でも不便である。さらに、この方法では部分的性質の特徴をみつけやすい不規則性の悪い位相点相互の類似性はわかりやすいが、不規則性のよい位相点では部分的性質が同じようなものになるため、それら相互の類似性を評価することは困難である。ところが実際に高次M系列を用いて擬似乱数を発生する際の初期値としては、さまざまな位相点の n タップルを用いる可能性がある。したがって不規則性のよしあしにかかわらず、任意の n タップルで表わされる位相点間の類似性を評価できることが望ましい。本論文はM系列の任意の二つの n タップルで表わされる位相点間の類似性を示す量として、新たに類似度というものを提案するものである。

2. 剰余多項式を用いた類似性の評価

あるM系列から位相差 d だけ遅れたM系列を得るためには (1) 式のようにM系列の特性多項式 $f(x)$ を法としたときの x^d の剰余多項式 $r(x)$ を求め、Fig. 1 に示すように $r(x)$ の係数が1となるシフトレジスタ

† 第24回計測自動制御学会学術講演会で発表 (昭60・7)

* 熊本大学工学部 熊本市黒髪 2-39-1

* Faculty of Engineering, Kumamoto University, Kumamoto

(Received October 20, 1986)

Fig. 1 A method of obtaining a delayed version of M-sequence
 (f_j : coefficient of characteristic polynomial,
 r_j : coefficient of remainder polynomial,
 $\{m_0\}$: original M-sequence, $\{m_d\}$: delayed M-sequence)

の段の出力間の排他的論理和をとればよい⁶⁾。

$$\begin{aligned} x^d &= h(x) \cdot f(x) + r(x) \\ &= r(x) \quad (\because f(x) = 0) \quad (1) \\ r(x) &= \sum_{j=0}^{n-1} r_j x^j \quad (r_j = 0 \text{ または } 1) \end{aligned}$$

また、もとのM系列と遅れたM系列が既知の場合、剰余多項式 $r(x)$ は連立方程式を解くことにより、一意に求めることができる⁹⁾。

これまでの研究では、剰余多項式 $r(x)$ の項数が少ないほどもとのM系列と遅れたM系列の部分的性質が類似することが知られている^{6)~7)}。また、 $r(x)$ の項数が多い場合でも、

$$r(x) = P(x)/Q(x)$$

($P(x), Q(x)$ はともに $(n-1)$ 次以下の多項式) という有理式の形で表わしたとき、 $P(x), Q(x)$ の項数がともに少ない場合には $r(x)$ の係数に規則性がみられ、もとのM系列と遅れたM系列の部分的性質が類似することがある⁶⁾。これらの場合はいずれも、遅れたM系列がもとの n 段のシフトレジスタのうちの少数の段の出力によって決定されることを意味し、このことがもとのM系列と遅れたM系列の部分的性質が類似する原因であると考えられてきた。しかし、もともになるM系列の初期 n タップルが不規則性のよいものである場合には、剰余多項式の項数が少ないときでも、遅れたM系列ともとのM系列の部分的性質が類似しないことがある。**Fig. 2** にその例を示す。この図は特性多項式 $f(x)$ 、もとのM系列の初期 n タップル m_0 、剰余多項式 $r(x)$ をそれぞれ、

$$f(x) = x^{89} + x^{38} + 1$$

$$m_0 = (0001010101 \ 1111110110 \ 1010000011$$

$$0000101000 \ 1111001000 \ 1011001100$$

$$1010101111 \ 1110000001 \ 000001100)$$

$$r(x) = x^7 + x + 1$$

(a) In the case of original M-sequence

(b) In the case of delayed M-sequence

Fig. 2 Autocorrelation function of M-sequence.
 The characteristic polynomial is $f(x) = x^{89} + x^{38} + 1$

としたときの、(a) もとのM系列、(b) 遅れたM系列の部分的自己相関関数 (サンプル数 1,000) である。この図より、もとのM系列の部分的性質は不規則性のよいものであるが、遅れたM系列の部分的性質はきわめて不規則性の悪いものであり、両者の間にはまったく類似性がみられないことがわかる。

以上の結果より、剰余多項式のみを用いてM系列の任意の二つの位相点における部分的性質の類似性を評価することは適当でないと考えられる。

3. 類似度による類似性の評価

本章では、まず、M系列の初期 n タップル中の 1, 0 の連がM系列の部分的性質に影響することを示す。例として、 $n = 2k$ (k : 正の整数) としたとき、つぎのような三つの n タップルより発生したM系列の部分的性質の類似性を考える。以下、 $1^i 0^j$ は 1 が i 個、0 が j 個続くことを示す記号とする。

$$m_a = (11 \dots 1) = (1^{2k})$$

$$m_b = (0 \dots 01 \dots 1) = (0^k 1^k)$$

$$m_c = (1010 \dots 10) = ((10)^k)$$

このとき、 m_b と m_c のどちらが m_a に類似しているかを比較してみる。まず、 n タップル中の 1, 0 の個数は m_b も m_c もそれぞれ k 個ずつで同じである。しかし、1, 0 の連を比べてみると、 m_a と m_b は長い連が続くという点で類似しているが、 m_c の連はすべて短く、 m_a とは類似していない。

つぎに、この三つの n タップルを初期値として発生したM系列の部分的性質を調べた結果を **Fig. 3** に示

Fig. 3 Autocorrelation function of M-sequence generated from three n -tuples. The characteristic polynomial is $f(x)=x^{98}+x^{27}+1$

す。ここで用いた特性多項式は

$$f(x)=x^{98}+x^{27}+1$$

であり、調べた部分的性質は各 n タップルより発生した M 系列 1,000 個の自己相関関数である。Fig. 3 より、初期値として m_a を用いた場合と m_b を用いた場合は自己相関関数に類似性がみられるが、 m_c を用いた場合は類似していないことがわかる。さらに同じ特性多項式、 n タップルを用いて Fig. 3 に示した以外の M 系列の部分的性質（連の自己相関関数、連の分布、Tausworthe 系列の分布）について調べた結果も同様のものであった。

以上の例より M 系列の n タップル m 中の 1, 0 の連が m を初期値として発生した M 系列の部分的性質に影響すると考えられる。そこで m 中の連に着目して、(2) 式のように q を定義する。

$$m=(m_0, m_1, \dots, m_{n-1})$$

$$q=(q_0, q_1, \dots, q_{n-2})$$

$$q_j=m_j \oplus m_{j+1} \quad (0 \leq j \leq n-2) \quad (2)$$

式中で $\oplus$ は排他的論理和を表す。したがって、連が継続しているならば、 $m_j=m_{j+1}$ より、 $q_j=0$ となり、

連の終端では $m_j \neq m_{j+1}$ となるので $q_j=1$ となる。

よって、 m 中の連の個数を l 個とすると q 中の 1 の個数は $(l-1)$ 個となる。また、 m を (3) 式のように表わすと、

$$m=(a_1^{r_1} a_2^{r_2} \dots a_l^{r_l}) \quad (3)$$

$$(a_i: 0 \text{ または } 1, a_i \neq a_{i+1}, r_i \geq 1)$$

q は (4) 式のようになり、

$$q=(0^{r_1-1} 0^{r_2-1} \dots 0^{r_l-1}) \quad (4)$$

(q 中の 0 の連の長さ)=(m 中の 1, 0 の連の長さ)-1 となっていることがわかる。このように (2) 式で定義した q における 1 の個数およびその間隔により、 m 中の 1, 0 の連の個数および長さを表わすことができる。

つぎに、 q における 1 の個数および 1 と 1 の間隔を以下のような方法で表わす。まず、 q より連続する k タップルを $(n-k)$ 個取り出し、(5) 式のように k タップルの各ビットに 2 のべき乗の重みをつけて得られる整数を $w_{k,j}$ とする。

$$w_{k,j} = \sum_{i=0}^{k-1} 2^i q_{i+j} \quad (0 \leq j \leq n-k-1) \quad (5)$$

このとき、取り出した k タップルは $(0^k) \sim (1^k)$ の 2^k 通りのうちのいずれかになるので、 $w_{k,j}$ は、

$$0 \leq w_{k,j} \leq 2^k - 1$$

のいずれかの値をとる。したがって、(5) 式より得られた $(n-k)$ 個の整数 $w_{k,j}$ の確率密度関数 $p(k, l)$ は (6) 式のようになる。

$$p(k, l) = \frac{w_{k,j} = l \text{ となる個数}}{n-k} \quad (6)$$

$$(0 \leq l \leq 2^k - 1)$$

この確率密度関数は q 中の 1 の個数や間隔が変わると異なる分布となるため、 $p(k, l)$ により m 中の連の分布を表わすことができると考えられる。

本研究で提案する類似度 Q はこの確率密度関数をもとに以下のように定義される。まず、M 系列の任意の二つの n タップル m_1, m_2 より (2) 式に従って q_1, q_2 を求める。つぎに、この q_1, q_2 より連続する k タップル ($1 \leq k \leq 16$) をとり出し、(5), (6) 式に従って $p_1(k, l), p_2(k, l)$ を得る。類似度 Q はこの二つの確率密度関数に共通部分の面積を求め、それにタップルの重みを乗じたものとして (7) 式のように定義される。

$$Q = \frac{\sum_{k=1}^{16} k \cdot \sum_{l=0}^{2^k-1} \min(p_1(k, l), p_2(k, l))}{\sum_{k=1}^{16} k} \quad (7)$$

(7) 式において、タップルの重みを乗じたのは、長いタップルにおける類似性を高く評価するためである。

また、タップルの長さを 16 までとしたのは本研究で

使用した計算機が1語16ビットのものであるからである。上式より、 m_1 と m_2 における1,0の連の分布が類似しているならば、 $p_1(k,l)$ と $p_2(k,l)$ の値に差がなくなり、両者に共通な部分の面積が増大し類似度 Q の値は大きくなる。そして $m_1=m_2$ となるとき、あるいは両者の連の分布がまったく同じとなるとき、 Q は最大値1をとる。逆に、 m_1 と m_2 にまったく類似性がみられないときは、 $Q=0$ となる。

上記の m_a, m_b, m_c の三つの n タプルを例にとると、 m_a と m_b の類似度 Q_1 および m_a と m_c の類似度 Q_2 は $n=98$ としたときそれぞれ

$$Q_1=0.89, \quad Q_2=0.00$$

となり、類似度を比較してみると m_a と m_b は類似しているといえるが、 m_a と m_c はまったく類似していないといえる。これは、Fig. 3のように実際にM系列を発生して部分的性質を求めた結果と一致している。

つぎに、さまざまな n タプルを位相原点としたときその $iT/360$ 位相点(T : M系列の周期, $0 \leq i \leq 359$)における n タプル m_p を取り、 m_0 と m_p の類似度を調べた結果をFig. 4およびFig. 5に示す。各図において、(a)は m_p を初期値として発生したM系列256個の不規則度¹⁰⁾、(b)は m_0 と m_p の類似度である。

まずFig. 4は特性多項式 $f(x)$ 、 m_0 をそれぞれ

$$f(x)=x^{127}+x^{48}+x^{12}+x+1$$

$$m_0=(10^7 10^{35} 10^{11})$$

とした場合である。ここでは m_0 特性M系列の初期 n

Fig. 4 Randomness of M-sequence and resemblance between initial n -tuple and delayed n -tuple. The characteristic polynomial is $f(x)=x^{127}+x^{48}+x^{12}+x+1$. The initial n -tuple at phase 0 is the characteristic M-sequence

Fig. 5 Randomness of M-sequence and resemblance between initial n -tuple and delayed n -tuple. The characteristic polynomial is $f(x)=x^{127}+x^{48}+x^{12}+x+1$

タプルである。Fig. 4より不規則度にみられる円分位相点($(T+1)/2'$ 位相点)における類似性が類似度にもみられることがわかる。また、 i が大きくなるほど類似性がみられなくなるといふ円分位相点の性質も類似度にもみられる。

つぎにFig. 5は同じ特性多項式を用い、 m_0 を

$$m_0=(1111111111 \ 1111110000 \ 0000001111 \\ 1000001111 \ 1111101111 \ 0000010001 \\ 1111110000 \ 1111001110 \ 1111000110 \\ 0000011111 \ 0000001110 \ 1001011000 \\ 0010100)$$

とした例である。この場合、位相原点に用いた n タプルが不規則性のよいものであるため(a)の不規則度は各位相点においてほぼ一定の値を示し、位相原点と類似しているかどうかは判断できない。しかし(b)の類似度では、Fig. 4の場合と同様に円分位相点において類似性がみられる。このFig. 5の場合について類似度の大きい $T/8$ 位相点と類似度の小さい $T/3$ 位相点の部分的性質を実際に求め、位相原点と比較した結果をFig. 6に示す。ここで調べた部分的性質は各位相点の n タプルより発生したM系列100個の自己相関関数である。この図より、 $T/8$ 位相点と位相原点の部分的性質は類似しているが、 $T/3$ 位相点の方には類似性がみられない。これは類似度の大きさから得られた結果と同じである。

以上の結果より、類似度 Q を用いることにより不規則性のよしあしにかかわらず、M系列の任意の二つの

Fig. 6 Autocorrelation function of M-sequence at several phases.

The characteristic polynomial is $f(x) = x^{127} + x^{48} + x^{12} + x + 1$

n タップル間の類似性を評価することができると考えられる。

4. あとがき

M系列の任意の n タップル間の類似性を表わす量と

して新たに、 n タップル中の 1, 0 の連に着目した類似度というものを提案した。そして、M系列を実際に発生してその部分的性質を求め、その類似性を調べるという従来の方法では類似性がわかりにくかった不規則性のよい n タップル間の類似性も、この類似度を用いることにより、定量的に表わすことができることを示した。また、類似度はM系列を実際に発生しなくても類似性を求めようとする二つの n タップルのみを用いて得ることができるという点でも便利である。

参 考 文 献

- 1) G. Marsaglia: Random Number Fall Mainly in the Planes, Proc. Nat. Acad. Sci., **61**, 25/28 (1968)
- 2) 津田: レーマー型合同法によらない乱数について, bit, **12**-9, 64/75 (1980)
- 3) 伏見, 手塚: 多次元分布が一様な擬似乱数列の生成法, 応用統計学, **10**-3, 151/163 (1982)
- 4) 柏木: M系列の部分的性質を考慮した一様乱数の発生, 数理解析研究所講究録 498, 140/152, 京都大学数理解析研究所 (1983)
- 5) 柏木, 原田: M系列の円分位相, 計測自動制御学会論文集, **18**-10, 999/1004 (1982)
- 6) 原田, 柏木: サンプルされたM系列の部分的性質, 計測自動制御学会論文集, **21**-3, 292/297 (1985)
- 7) H. Kashiwagi and H. Harada: On Partial Properties of M-Sequence, Proc. 9th IFAC Congress Held in Budapest, Hungary, Vol. 10, 150/155 (1984)
- 8) A.C. Davis: Delayed Versions of Maximal-Length Linear Binary Sequences, Electron. Lett., **1**-3, 61/63 (1965)
- 9) 原田, 柏木: M系列の n タップル間の位相差, 計測自動制御学会論文集, **20**-6, 542/547 (1984)
- 10) 柏木, 小橋, 原田: M系列の部分的不規則性の評価, 計測自動制御学会論文集, **23**-8, 812/815 (1987)