円分位相点における M 系列の部分的性質の類似性

原 田 博 之*・柏 木 潤*

Resemblance of Partial Properties of M-Sequence at Cyclotomic Phase

Hiroshi HARADA* and Hiroshi KASHIWAGI*

Cyclotomic phase is a useful concept in studying the phase properties of an M-sequence. This paper shows that the resemblance of the partial properties of an M-sequence at cyclotomic phases is clearly explained by use of sampling 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

M系列の部分的性質の良否は、高次M系列を用いて擬似乱数を発生するときの初期値の選択の際に重要な問題となる^{1),2)}。M系列の部分的性質を調べるときに有用な概念として、筆者らは先に円分位相（ある初期 n タップルを基準としてそれから $(N+1)/2^j$ 離れた位相点、 N : M系列の周期、 j : 正の整数）という概念を提案し、M系列の部分的性質が円分位相点において類似することを示した¹⁾。文献 1)において、部分的性質が類似する原因として、円分位相点における剰余多項式の項数が少ないことがあげられている。しかし、剰余多項式の項数が少ない場合でも部分的性質が類似しない例³⁾や、逆に項数が多い場合でも部分的性質が類似する例⁴⁾が報告されており、剰余多項式の項数のみでM系列の部分的性質の類似性を論ずるのは適当でないと考えられる。

そこで本研究では、M系列を一定間隔でサンプルして得られる系列の性質をもとに、円分位相点における部分的性質の類似性を論じ、特性M系列⁵⁾の場合とそれ以外の初期値より発生したM系列では円分位相点の類似性が異なることを示す。つぎに、実際に特性M系列の初期 n タップルとすべて1からなる n タップルのそれぞれを位相原点とした場合について各位相点におけるM系列の部分的性質の類似性を調べ、この議論が正しいことを示す。

2. M系列のサンプリングに関する性質を用いた円分位相点における部分的性質の類似性の説明

以下、M系列の位相点を表わすのに、特性M系列の初期 n タップルを位相原点とした、いわば絶対的位相点を特性位相点と称して、任意の n タップルを位相原点としたときの位相点と区別することにする。

はじめに、特性M系列の初期 n タップルを位相原点とする場合を考える。 n 次M系列 $\{a_i\}$ を一定間隔 s でサンプルして得られる系列 $\{a_{si}\}$ は、 $s=2^j$ (j : 正の整数) ならば $\{a_i\}$ と同じ特性多項式をもつM系列となることが知られており⁶⁾、特に、 $\{a_i\}$ が特性M系列の場合は、

$$\{a_{si}\} = \{a_i\}$$

となる⁶⁾。上式において、等号は項ごとに等しいことを表わす。ここで、 $s=2$ の場合について、 $\{a_{2i}\}$ と $\{a_i\}$ の関係を示したのが Fig. 1 である。この図より、 $\{a_i\}$ の $(N+1)/2$ 特性位相点は特性 M 系列の初期 n タップル付近をサンプルして得られたものであることがわかる。このため、位相原点と $(N+1)/2$ 特性位相点の部分的性質が類似すると考えられる。さらに $s=4, 8, 16, \dots$ の場合についても同様に、 $\{a_i\}$ の $k \cdot (N+1)/s$ 特性位相点 ($1 \leq k \leq s-1$) は $\{a_i\}$ の位相原点付近を s 個ごとにサンプルしたものであるため、部分的性質が類似すると考えられる。また位相原点において不規則性の悪い系列が続く長さを L とすると、 $k \cdot (N+1)/s$ 特性位相点 ($s=2^j$, j : 正の整数) における

Fig. 1 Relation between original M-sequence and sampled M-sequence when sampling period is 2

* 熊本大学工学部 熊本市黒髪 2-39-1

* Faculty of Engineering, Kumamoto University, Kumamoto

(Received July 3, 1987)

不規則性の悪い系列の長さはほぼ $L/2^j$ となり、 j の値が大きくなるほど、その長さは短くなる。このことは、文献1)に示される円分位相点における部分的性質の類似性が j が大きくなるほど小さくなることと対応すると考えられる。

つぎに、位相原点となる n タップル $\mathbf{a}_d$ が特性M系列の初期 n タップル $\mathbf{a}_0$ 以外の場合について、上記と同様の方法により、部分的性質の類似性を考える。このとき $\mathbf{a}_d$ と $\mathbf{a}_0$ の位相差を d とすると、 $s=2$ の場合、Fig. 1 よりもとのM系列 $\{a_i\}$ の $\mathbf{a}_d$ 付近をサンプルしたのは $d/2$ 特性位相点および $(d+N)/2$ 特性位相点である。したがって、位相原点となる n タップルを $\mathbf{a}_0$ としたときの $\mathbf{a}_0$ とその円分位相点との関係は、 $s=2$ のときの $\mathbf{a}_d$ と d/s 特性位相点および $(d+N)/s$ 特性位相点の関係となる。同様に $s=2^j (j=2, 3, 4, \dots)$ の場合については、 $(d+k \cdot N)/s$ 特性位相点 ($0 \leq k \leq s-1$) が $\mathbf{a}_d$ と部分的性質が類似した位相点となる。

3. 各位相点における部分的性質の類似性の実測結果

実際に、M系列のさまざまな位相点における部分的性質の類似性を調べ、前章で述べたように部分的性質が類似する位相点の位置が初期 n タップルによって異なることを確認する。まず、特性M系列の初期 n タップルおよびすべて1からなる n タップルを位相原点とし、1/400 位相点ごとに位相原点との類似度³⁾を求めた結果を Fig. 2 に示す。ここで、用いた特性多項式 $f(x)$ は

$$f(x) = x^{127} + x^{22} + x^{18} + x + 1$$

(a) n -tuple at phase 0 is the initial n -tuple of characteristic M-sequence

(b) n -tuple at phase 0 is the n -tuple containing all 1

Fig. 2 Resemblance between initial n -tuple and delayed n -tuple where the characteristic polynomial is $f(x) = x^{127} + x^{22} + x^{18} + x + 1$ and phase step is $N/400$

である。Fig. 2(a)より、特性M系列の初期 n タップルを位相原点とした場合は、 $k \cdot (N+1)/2^j$ 特性位相点 ($j=1, 2, 3, 4; 1 \leq k \leq 2^j-1$) において類似度の値が大きいことがわかる。また、 j の値が小さいほど、類似度の値は大きく、円分位相点の特徴をよく表わしている。ところが、Fig. 2(b)のすべて1からなる n タップルを位相原点とした場合は、すべての位相点において類似度の値が小さく、部分的性質の類似はみられない。

つぎに、Fig. 2 の例で、特性M系列の初期 n タップルとすべて1からなる n タップルとの位相差を d とするとき、 $d/2^j$ 特性位相点 ($j=1, 2, 3$) の n タップルを位相原点とし、1/400 位相点ごとにすべて1からなる n タップルとの類似度を求めた結果を Fig. 3 に示す。この図より、 $d/2^j$ 特性位相点を位相原点とした場合は、 $k \cdot (N+1)/2^j$ 特性位相点 ($0 \leq k \leq 2^j-1$) において、すべて1からなる n タップルとの類似度が大きいことがわかる。また、 j の値が小さいほど、類似度の値が大きいことがわかる。このことは、前章で述べた $\mathbf{a}_d$ と部分的性質が類似する位相点が $(d+k \cdot N)/2^j$ 特性位相点となることと、対応している。以上の結果より、特性M系列の初期 n タップルを位相原点とした

(a) $s=2$

(b) $s=4$

(c) $s=8$

Fig. 3 Resemblance between the n -tuple containing all 1 and delayed n -tuple where the characteristic polynomial is $f(x) = x^{127} + x^{22} + x^{18} + x + 1$ and phase step is $N/400$. The phase difference between the initial n -tuple of characteristic M-sequence and the n -tuple at phase 0 is d/s

ときと、その他の n タプルを位相原点としたときでは部分的性質が類似する位相点の位置が異なり、前章の議論が正しいことが示された。

4. あとがき

M系列を一定間隔でサンプルして得られる系列の性質を用いて、円分位相点におけるM系列の部分的性質の類似性の説明を試みた。そして、特性M系列とその他の n タプルより発生したM系列では円分位相点における部分的性質の類似性が異なることを示し、特性M系列以外の n タプルより発生したM系列における部分的性質の類似する位相点の位置を示した。さらに、実際にM系列の各位相点における部分的性質の

類似性を調べた結果、このことが正しいことが示された。

参考文献

- 1) 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)
- 2) 原田, 柏木: M系列を用いる乱数発生, 計測自動制御学会論文集, **23**-8, 806/811 (1987)
- 3) 原田, 柏木: M系列の部分的性質の類似性の評価, 計測自動制御学会論文集, **23**-8, 816/820 (1987)
- 4) 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)
- 5) 柏木: M系列再発見, 計測と制御, **20**-2, 236/245 (1981)
- 6) S. W. Golomb: Shift Register Sequences, Holden-Day (1967)