

## M 系列に基づく一様乱数の多次元ラソダムネスの検定

岡山理大 山本英二 ( Eiji Yamamoto )

林野高 菅野長武 ( Osamu Sugano )

### 1. M 系列に基づく一様乱数の発生法

周期  $N$  の 2 値系列の内 1 周期では等頻度性や無系列相関性を持つ系列に M 系列がある。M 系列はその他にも良い性質を持つことが理論的に知られている。M 系列を使って  $[0,1)$  の一様乱数を作る方法に Tausworthe 法 (1965) がある。彼の方法は  $P$  次の原始多項式を特性多項式とする漸化式を用いた周期  $N=2^P-1$  の M 系列  $\{a_i\}$  を発生させ、その相続く  $l$  ( $\leq P$ ) 個の要素を並べて  $l$  ビットの 2 進小数系列 (これを横型系列という) を作るものである。

$$(1) \quad w_t = 0.a_{\sigma t+r-1} a_{\sigma t+r-2} \cdots a_{\sigma t+r-l}$$

( $\sigma$ ;  $\geq l$ ,  $N$  と素  $r$ ; 初期位相)

このとき  $\{w_t\}$  は周期  $N$  を持ち、 $k$  ( $\leq \frac{P}{l}$ ) 次均等分布、平均・分散の不偏性や無系列相関性を高い精度で持つことが知

られている。しかし、この方法は発生速度が遅い欠点を持つ。

この発生速度を高速化するために、M系列の位相をずらしたものを各ビットに配する縦型系列と呼ばれる2進小数系列

$$(2) \quad w_t = 0.a_{t+\tau_1} a_{t+\tau_2} \dots a_{t+\tau_\ell}$$

を発生させる Lewis & Payne 法 (1973) や、その改良版

Arvillias & Maritsas 法 (1978) が考案されたが彼らの系列は横型系列の持つ良い性質 (k 次均等分布) を失っていた。

そこで伏見手塚 (1981)、伏見 (1983) は縦型系列の高速発生算法を利用して次の横型系列を発生させる方法を提案した。

3 次原始多項式  $f(x) = x^{521} + x^{32} + 1$  を特性多項式とする漸化式

$$(3) \quad a_t \equiv a_{t-521} \oplus a_{t-32} \quad (\oplus \text{ は繰り上りなしの和})$$

で作られる周期  $N = 2^{521} - 1$  の M 系列に基づく横型系列を次の

$$(4) \quad w_t = 0.a_{32(t-1)+1} a_{32(t-1)+2} \dots a_{32(t-1)+31}$$

$$(P=521, \ell=32, [P/\ell]=16)$$

算法で発生させる。

1.  $a_1, \dots, a_{521}$  の値を任意に 0 または 1 とする。(全て 0 とはしない)
2. (3) を用いて  $a_t$  ( $t=522, \dots, 16672$ ) を発生させる。

3. (4) を用いて  $w_t$  ( $t=1, \dots, 521$ ) を発生させる。

4.  $w_t$  ( $t \geq 522$ ) を漸化式:

$$(5) \quad w_t = w_{t-521} \oplus w_{t-32}$$

で発生する。

この算法は32とNが互いに素なので、M系列  $\{a_t\}$  を間隔32で抽出して得られる系列  $\{a_{32t}\}$  は元のM系列をある位相だけシフトしたものになっているので、初期位相を  $i$  とすれば

$$(6) \quad a_{32t+i} \equiv a_{32(t-521)+i} \oplus a_{32(t-32)+i} \\ (i=1, \dots, 31)$$

の漸化式が成り立つので (5) が成立することを利用したものである。

## 2. 統計的検定

伏見手塚はこうして発生させた彼らのM系列に基く一様乱数は200万個の部分列についても多くの統計的検定項目: 度数検定・系列検定・ポーカー検定・連の検定・ギャップ検定に合格すると報告している。1周期にわたればk次均等性を持つので部分列でもk次均等性の検定に合格すると思われるが、k次独立性についてはどうであろうか。そこで我々は伏見手塚の一様乱数系列に2次元  $d^2$  検定, 我々の提案した

3次元 Random Distance 検定 (1981), 菅野の提案した  
4次元 Random Manhattan Distance 検定 (1982) を行った。  
即ち、

$$(7) \quad \begin{aligned} d_2^2 &= \sum_{j=1}^2 (U_{1j} - U_{2j})^2 \\ d_3^2 &= \sum_{j=1}^3 (U_{1j} - U_{2j})^2 \\ MD_4 &= \sum_{j=1}^4 |U_{1j} - U_{2j}| \end{aligned} \quad \left( \begin{array}{l} \perp (U_{ij}) \\ U_{ij} \sim U(0,1) \\ i=1,2 \quad ; j=1,\dots,4 \end{array} \right)$$

の分布を利用した検定である。  $d_2^2, d_3^2$  は 2次元、3次元バクトル空間の2点間のユークリッド距離の2乗である。

$MD_4$  は 4次元バクトル空間の2点間のマンハッタン距離である。  
 $d_4^2$  が考えられるがその分布関数は初等関数の範囲で表現できない。  
 $d_2^2, d_3^2, MD_4$  の分布関数  $F_2, F_3, F_4$  は表1となる。この分布関数を用いて  $\chi^2$  検定を行うことになる。

### 3. 計算結果

ここでは代見手塚の報告 (1981) と比較が可能となる様、彼らの発生させた一様乱数系列とまったく同一のものを利用した。

$d_2^2$ -検定は、相続く4個の乱数で一つの  $d_2^2$  を作りこれを500回使って一つの  $\chi^2$  値を計算した。区間数は10とし、各区間がほぼ等確率 0.1 となるように区間端点は求めた。

この $\chi^2$ 値を100回用いて次のKolmogorov-Smirnov 検定統計量を計算した。

$$\begin{aligned}
 KS+ &= \sup_t \{F_n(t) - F(t)\} \\
 (8) \quad KS- &= \sup_t \{F(t) - F_n(t)\} \\
 KS &= \sup_t |F_n(t) - F(t)|
 \end{aligned}
 \quad \begin{array}{l} (F(t); \text{理論分布関数}) \\ (F_n(t); \text{経験分布関数}) \end{array}$$

これを10回くり返した。使用乱数の数は  $4 \times 500 \times 100 \times 10 = 200$  万回である。

$d_3^2$ -検定は相続く6回の乱数で一つの $d_3^2$ を作り、これを334回使って一つの $\chi^2$ 値を計算する。区間数は10で、各区間、ほぼ等確率である。この $\chi^2$ 値を100回用いてK-S検定統計量を計算した。これを10回くり返す。 $6 \times 334 \times 100 \times 10 = 200.4$  万回の乱数を使用した。

$MD_4$ -検定は相続く8回の乱数で一つの $MD_4$ を作りこれを250回使って一つの $\chi^2$ 値を計算する。区間数は同じ10である。等確率となるようにしておく。この $\chi^2$ 値を100回用いてK-S検定統計量を計算する。これを10回くり返す。 $8 \times 250 \times 100 \times 10 = 200$  万回の乱数を使用した。

計算結果を表2に示されている。 $d_3^2$ -検定の $KS+$ 、 $d_3^2$ -検定の $KS-$ で5%有意なものが10回中、各1回、 $MD_4$ -検定では5%有意なものが $KS+$ 、 $KS$ で各10回中2回

でている。MD<sub>4</sub>-検定では、不合格と言えようである。

伏見・千塚のM系列に基づく一様乱数の200万個程の部分系列について、多次元ランダムネスについての統計的検定に不合格になる部分系列が存在するとの知見を得た。

#### REFERENCES

- [1] R.C.Tauswerth(1965), Mathematics of Computation, 14, 201-209.
- [2] T.G.Lewis & W.H.Payne(1973), J.ACM, 21, 456-468.
- [3] A.C.Arwillias & D.G.Maritsas(1978), J.ACM, 25, 675-686.
- [4] 伏見正則 & 千塚 集 (1981), 応用統計学, 10, 151-163.
- [5] E.Yamamoto & O.Sugano(1981), J. Japan Statist. Soc., 11, 15-25.
- [6] O.Sugano(1982), J. Japan Statist. Soc., 12, 113-124.
- [7] 伏見正則(1983), 情報処理, 24, 367-371.

## 表 1

$$F_2(\alpha^2) = \begin{cases} \pi\alpha^2 - \frac{8}{3}\alpha^3 + \frac{1}{2}\alpha^4 & (0 \leq \alpha^2 \leq 1) \\ \frac{1}{3} + (\pi - 2)\alpha^2 + 4(\alpha^2 - 1)^{1/2} + \frac{8}{3}(\alpha^2 - 1)^{3/2} - \frac{1}{2}\alpha^4 - 4\alpha^2 \sec^{-1} \alpha & (1 \leq \alpha^2 \leq 2) \end{cases}$$

$$F_3(\alpha^2) = \begin{cases} \frac{4}{3}\pi\alpha^3 - \frac{3}{2}\pi\alpha^4 + \frac{8}{5}\alpha^5 - \frac{1}{6}\alpha^6, & (0 \leq \alpha^2 \leq 1) \\ \left(\frac{5}{2}\pi + \frac{43}{30}\right) - 6(\alpha^2 - 1)^{1/2} + \left(3\pi + \frac{7}{2}\right)(\alpha^2 - 1) - \frac{8}{3}\pi\alpha^3 - 10(\alpha^2 - 1)^{3/2} \\ + \frac{5}{2}(\alpha^2 - 1)^2 - \frac{16}{5}(\alpha^2 - 1)^{5/2} + \frac{1}{3}(\alpha^2 - 1)^3 + 6\alpha^4 \sec^{-1} \alpha, & (1 \leq \alpha^2 \leq 2) \\ \left(\frac{23}{2}\pi - \frac{343}{30}\right) + 14(\alpha^2 - 2)^{1/2} + \left(9\pi - \frac{21}{2}\right)(\alpha^2 - 2) + 10(\alpha^2 - 2)^{3/2} \\ + \left(\frac{3\pi - 5}{2}\right)(\alpha^2 - 2)^2 + \frac{8}{5}(\alpha^2 - 2)^{5/2} - \frac{1}{6}(\alpha^2 - 2)^3 \\ - 2(3\alpha^4 + 6\alpha^2 - 1) \sec^{-1} \sqrt{\alpha^2 - 1} + 8\alpha^3 \sec^{-1}(\alpha^2 - 1) - \frac{8}{3}\pi\alpha^3 & (2 \leq \alpha^2 \leq 3) \end{cases}$$

$$F_4(x) = \begin{cases} 0 & (x \leq 0) \\ 2x^4/3 - 8x^5/15 + 2x^6/15 - 4x^7/315 + x^8/2520 & (0 \leq x \leq 1) \\ 641/2520 + 5(x-1)/7 + 37(x-1)^2/90 - 19(x-1)^3/45 - 5(x-1)^4/12 \\ + 5(x-1)^5/9 - 19(x-1)^6/90 + (x-1)^7/35 - (x-1)^8/840 & (1 \leq x \leq 2) \\ 115/126 + 32(x-2)/105 - 2(x-2)^2/5 + 8(x-2)^3/45 + (x-2)^4/9 \\ - 8(x-2)^5/45 + 4(x-2)^6/45 - 2(x-2)^7/105 + (x-2)^8/840 & (2 \leq x \leq 3) \\ 2519/2520 + (x-3)/315 - (x-3)^2/90 + (x-3)^3/45 - (x-3)^4/36 \\ + (x-3)^5/45 - (x-3)^6/90 + (x-3)^7/315 - (x-3)^8/2520 & (3 \leq x \leq 4) \\ 1 & (4 \leq x) \end{cases}$$

表2

 $d_2^2$ -test

| NO. | KS+    | KS-     | KS      |
|-----|--------|---------|---------|
| 1   | .03362 | .06147  | .06147  |
| 2   | .01841 | .09032  | .09032  |
| 3   | .08069 | .04155  | .08069  |
| 4   | .03325 | .05084  | .05084  |
| 5   | .08597 | .03126  | .08597  |
| 6   | .07982 | .05318  | .07982  |
| 7   | .04177 | .04314  | .04314  |
| 8   | .00819 | .14688* | .14688* |
| 9   | .07130 | .02157  | .07130  |
| 10  | .03642 | .06422  | .06422  |

 $d_3^2$ -test

| NO. | KS+     | KS-    | KS     |
|-----|---------|--------|--------|
| 1   | .02058  | .08057 | .08057 |
| 2   | .12890* | .04410 | .12890 |
| 3   | .07869  | .01146 | .07869 |
| 4   | .04691  | .04684 | .04691 |
| 5   | .08452  | .03011 | .08452 |
| 6   | .06874  | .05620 | .06874 |
| 7   | .05353  | .06379 | .06379 |
| 8   | .03924  | .04565 | .04565 |
| 9   | .01309  | .07439 | .07439 |
| 10  | .05776  | .08293 | .08293 |



MD<sub>4</sub>-test

| NO. | KS+     | KS-    | KS      |
|-----|---------|--------|---------|
| 1   | .06708  | .06241 | .06708  |
| 2   | .03183  | .06278 | .06278  |
| 3   | .08216  | .04143 | .08216  |
| 4   | .08638  | .04165 | .08638  |
| 5   | .03336  | .08364 | .08364  |
| 6   | .14487* | .01603 | .14487* |
| 7   | .13908* | .00041 | .13908* |
| 8   | .03075  | .03361 | .03361  |
| 9   | .04434  | .07716 | .07716  |
| 10  | .06521  | .04623 | .06521  |