1997年度日本オペレーションズ・リサーチ学会
秋季研究発表会

素数の法を有する乗算合同型擬似乱数生成法の系列相関絶対値とスペクトル検定尺度との関連の推測

01207060 早稲田大学 *坂本宗隆 SAKAMOTO Munetaka
01603200 早稲田大学 森戸 晋 MORITO Susumu

1 はじめに

擬似乱数は，無作為標本抽出や離散事象シミュレーションや計算機アルゴリズム評価用データ作成などに用いられる。無作為標本抽出では，乱数さいをふったり乱数表をひいたりすれば済むこともあるが，計算機によって擬似乱数を生成してもよい。離散事象シミュレーションやアルゴリズム評価用データ作成では，計算機によって擬似乱数を生成するのが普通である。計算機による擬似乱数生成の方法として広く普及しているのは—いうまでもなく—乗算合同型擬似乱数生成法(乗算合同法)である。乗算合同法のなかでは，法が素数であるようなものがよいと認識されている [8]。法が素数であるような乗算合同法の法の値を決める際には，法の値を，計算機で表現されうる最大の整数値にできるだけ近い素数の値とするだけでよいものと考えられることが多い。

法の値が定められたとき，乗算合同法によって得られる数列が，真の乱数列に近いかどうかということは，乗数の値の影響を受ける

乗算合同法を特殊形として含む線形合同法に関する Donald E. Knuth [4, 第3.6節] の原則は，乗算合同法の乗数の値を決める際に，数列の全周期にわたる系列相関（系列相関係数と呼ばれることもある）の絶対値の上界を大きくしない必要性を指摘すると同時にスペクトル検定の結果をよくする必要性をも示唆している。

ところが，素数の法を有する乗算合同法に関する Knuth 以後の研究のなかには，乗算合同法数列が真の乱数に近いかどうかということを測る尺度として，系列相関絶対値（またはその上界）を考慮しないでスペクトル検定尺度を考慮するもの [3][8] もある。

このようなわけで，本報告では，スペクトル検定尺度の値がよければ系列相関絶対値（またはその上界）が小さいという命題の反証を探す数値実験の結果を示すことを目的とする。

2 法が素数の乗算合同法

乗算合同法は，三つの整数: 法 m $(m > 2)$, 乗数 a $(0 < a < m)$, 初期値 X_0 $(0 < X_0 < m)$ によって定まる。範囲 $[1, m-1]$ にある整数の列 $\{X_n \mid n \geq 0\}$ は漸化式 $X_n = aX_{n-1} \bmod m$ によって得られる。区間 $(0,1)$ 上の，対応する数列 $\{U_n \mid n \geq 0\}$ は，正規化 $U_n = X_n/m$ によって得られる。

2.1 周期

乗算合同法による数列 $\{X_n \mid n \geq 0\}$ および $\{U_n \mid n \geq 0\}$ は等しい周期 $\lambda \stackrel{\text{def}}{=} \min\{l \geq 1 \mid X_{n+l} = X_n \text{ for each } n \geq 0\}$ を有する。法 m が素数であるとき，乗数 a の値をどのように選んでも周期 λ の値は $m-1$ 以下である: 最大周期は $m-1$ である。周期が最大周期に等しくなるのは，乗数 a が，法 m の原始根である場合に限られる。

2.2 スペクトル検定尺度

乗算合同法によって得られる数列には，連続 t 項の組 $(\tilde{U}_0, \tilde{U}_1, \ldots, \tilde{U}_{t-1})$, $(\tilde{U}_1, \tilde{U}_2, \ldots, \tilde{U}_t), \ldots$ を t 次元単位超立方体の中の点とみなしたとき，これらの点がすべて，等しい距離をおいて平行に並ぶ比較的少ない $(t-1)$ 次元超平面の上にあるという欠陥がある。法が m, 乗数が a であるような乗算合同法に対するスペクトル検定では，このような超平面から成るあらゆる集合に含まれる隣り合う超平面の間の距離のうちで最も長いもの $d_t(a,m)$ が短ければ短いほど，連続 t 項が t 次元空間に一様に分布している度合が高いと考える。

法 m が与えられているとき，乗数 a をどのように選んでも，$d_t(a,m)$ を不等式 $d_t(a,m) \geq d_t^*(m) \stackrel{\text{def}}{=} \gamma_t^{-1/2} m^{-1/t}$ の右辺より小さくすることはできない(ただし，γ_t は，Hermite (エルミート) の定数である)[1]。

T 次元までの空間での検定をし，距離 $d_t(a,m)$ とその下界 $d_t^*(m)$ とによって定まる尺度 $M(T) = \min_{2 \leq t \leq T} d_t^*(m)/d_t(a,m)$ を考慮する [3]。尺度 $M(T)$ の値は，$(0,1]$ の範囲にあるが，大きいほうがよい。

[1]距離 $d_t(a,m)$ の下界 $d_t^*(m)$ の値は $t \leq 8$ についてしかわかっていないが，$8 < t \leq 24$ については，John Leech [6] の計算した，t 次元最密格子パッキングの中心密度 (center density) に対する C. A. Rogers の上界値を用いて $d_t^*(m)$ のかなり良い下界値を算出することができる。文献 [1, 表 1.2] に示されている，中心密度に対する下界値を利用すると，Rogers の上界に基づく，$d_t^*(m)$ の下界値から算出される $M(T)$ の推定値 (下界値) の相対誤差が，$8 < T \leq 24$ のときに6.5％未満であることがわかる。

2.3 系列相関絶対値の上界

数列 $\{U_n \mid n \geq 0\}$ の，(遅れ1の) 系列相関

$$c_1 = \frac{(m-1)\sum_{n=0}^{m-2} U_n U_{n+1} - \left(\sum_{n=0}^{m-2} U_n^2\right)}{(m-1)\sum_{n=0}^{m-2} U_n^2 - \left(\sum_{n=0}^{m-2} U_n^2\right)}$$

の絶対値が大きい場合，項 U_n と項 U_{n+1} とが独立であるとみなすことはできない。したがって，系列相関の絶対値が小さいことが必要である [4, 第3.3.3節]。

系列相関 c_1 は，Dedekind 和 $\sigma(a,m)$ を含む式

$$c_1 = \frac{m\,\sigma(a,m)}{(m-2)(m-1)} \tag{1}$$

で表される [2, 式 (4.12)][2]。

Dedekind 和の絶対値 $|\sigma(a,m)|$ の上界 [5, 第4節] から，法 m と乗数 a との最大公約数を求めるユークリッド互除法における商 $q_1, q_2, \ldots, q_t$ によって表される上界 $\sum_{j=1}^{t} q_j - 1$ が得られる。ゆえに，系列相関絶対値 $|c_1|$ には，不等式

$$|c_1| \leq \frac{m\left(\sum_{j=1}^{t} q_j - 1\right)}{(m-2)(m-1)}$$

の右辺で表される上界が存在する。

2.4 系列相関絶対値

Dedekind 和 $\sigma(a,m)$ は，

(i) 法 m と乗数 a との最大公約数を求めるユークリッド互除法における商を $q_1, q_2, \ldots, q_t$

(ii) 法 m に関する乗数 a の逆元を a'

と記すとき，

$$\sigma(a,m) = \frac{a+a'}{m} - 2 + (-1)^t + \sum_{j=1}^{t} (-1)^{j+1} q_j$$

と表される (Knuth [4, 2nd ed., 第3.3.3節，定理D] 参照)。法 m が素数である乗算合同法を考えているので，法 m および乗数 a は互いに素である。したがって，逆元 a' は，拡張ユークリッド互除法 [4, 第4.5.2節，算法X] の実行結果から整数演算だけによって容易に求められる。商 $q_1, q_2, \ldots, q_t$ は，もちろん，拡張ユークリッド互除法によって計算される。したがって，系列相関絶対値は，式 (1) によって計算される。

[2] Dedekind 和 $\sigma(a,m)$ の定義については，Knuth [4] による一般Dedekind 和の定義を，整数 c の値を零として参照。

3 スペクトル検定尺度の値がよい乗数に関する系列相関絶対値およびその上界

Fishman, Moore [3] にならい，2次元から6次元までにおけるのスペクトル検定の尺度 $M(6)$ の値を考慮，

(i) 数列の周期が最大になり (第2.1節)

(ii) 尺度 $M(6)$ が0.8以上の値をとる (第2.2節)

すべての乗数をよい乗数とみなす (ただし，法 m の値は，実験結果の一般性が失われない範囲で小さい素数の値とする)。よい乗数に関する系列相関絶対値上界 (第2.3節) の値を計算し，その最大値，最小値，中央値，平均値に基づいて，スペクトル検定尺度の値がよい乗数に関する系列相関絶対値上界は小さいという命題が成り立つかどうか考える。系列相関絶対値 (第2.4節) についても同様の実験を行い，命題が成り立つかどうか考える。(実験結果を，発表会で示す。)

参考文献

[1] Conway, J. H., and Sloane, N. J. A.: *Sphere Packings, Lattices and Groups* (Springer, New York, 1988).

[2] Dieter, U., and Ahrens, J.: "An exact determination of serial correlations of pseudo-random numbers," *Numerische Mathematik* **17** (1971), 101–123.

[3] Fishman, G. S., and Moore, L. R., III: "An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31}-1$," *SIAM J. Scientific Statistical Comput.* **7** (1986), 24–45.

[4] Knuth, D. E.: *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, 2nd ed., (Addison-Wesley, Reading, MA, 1981).

[5] Knuth, D. E.: "Notes on generalized Dedekind sums," *Acta Arithmetica* **33** (1978), 297–325.

[6] Leech, J.: "Notes on sphere packings," *Canadian J. Mathematics* **19** (1967), 251–267.

[7] Marsaglia, G., and Zaman, A.: "Some portable very-long-period random number generators," *Comput. Physics* **8** (1994), 117–121.

[8] Park, S. K., and Miller, K. W.: "Random number generators: Good ones are hard to find," *Commun. ACM* **31** (1988), 1192–1201; correspondence, idem **36** (1993), No. 7, 105–110.