1995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

# 数列の系列相関の絶対値が小さい乗算合同型疑似乱数生成法の探索

02201770 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

計算機による疑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—乗算型疑似乱数生成法(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値とするだけでよいものと考えられることが多い; また, 乗数の値を決める際には,

(i) 得られる数列の周期が最大になり,

(ii) その乗算合同法に対するスペクトル検定の結果がよくなり,

(iii) その乗算合同法が, ある効率的なアルゴリズム [9] によって正しく実現される

ように乗数の値を選ぶことの大切さが知られている [8].

二より大きな素数 $p$ は, $(p-1)/2$ もまた素数であるとき, 安全素数と呼ばれる [7]. 法の値は, 計算機で表現されうる最大の整数値にできるだけ近い安全素数の値とするほうがよい [7]. その理由は,

(i) 乗数の値の候補となる値のうちの約半数が, 最大周期条件を満たすこと,

(ii) 最大周期数列から得られる重複しない $t$ 項の組の列の周期が, ($t$ の値に, まれな例外があることを別にすれば) 最大周期の二分の一以上になること

の二つである [7].

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 [5, 第3.6節] の原則は, 乗算合同法の乗数の値を決める際に, スペクトル検定の結果をよくする必要性を指摘すると同時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) の絶対値を大きくしない必要性をも示唆している.[1]

本報告の目的は, 32 ビット計算機で用いられる乗算合同法の法の値と乗数の値とを選定することである. すなわち, 法の値を, $2^{31}$ より小さな最大の安全素数とし,

(i) 数列の周期が最大になり,

(ii) スペクトル検定の結果がよくなり,

(iii) 系列相関の絶対値が小さくなり,

(iv) その乗算合同法が, 効率的なアルゴリズム [9] によって正しく実現される

ように乗数の値を選ぶことが目的である.

[1] さらにまた, 全周期にわたる二次元差異を大きくしない必要性をも示唆している. 二次元差異は, 準乱数列から得られる二次元点列 (重複しない2項の組の列) の評価尺度のひとつである. 多次元数値積分や全域最適化には, 疑似乱数よりも準乱数のほうが適している [1, 第6.2節]. 本報告では, 疑似乱数列の評価にも, その数列から得られる点列の評価にも, 二次元差異を用いる必要がないという立場をとる. 疑似乱数生成法の評価に二次元差異を用いる必要がないかどうかということ, あるいは, 無作為標本抽出や離散事象シミュレーションなどに疑似乱数と準乱数とのうちのどちらを用いるべきかということはまだ疑問であろうと推測する.

## 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

#### 2.1.1 数列の周期

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 $\lambda$ 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.

法 $m$ が安全素数である場合, つまり, $m-1$ の素因数分解が $2 \cdot [(m-1)/2]$ と表される場合を考える. 1でも $m-1$ でもない乗数のうちの半数以上が, 法 $m$ の原始根であるので, 最大周期数列をもたらす [7].

#### 2.1.2 最大周期数列から得られる重複しない $t$ 項の組の列の周期

最大周期数列から得られる重複しない $t$ 項の組の列の周期は, 最大周期を, $t$ とその最大周期との最大公約数で割った値に等しい. ゆえに, 最大周期に素因数は少ないほうがよい. 最大周期 $m-1$ の素因数の個数は, 法 $m$ が安全素数であるとき, 最も小さく, 二になる. このとき, 最大周期数列から得られる重複しない $t$ 項の組の列の周期は, $t$ が $(m-1)/2$ で割り切れない限り, 最大周期の二分の一 $(m-1)/2$ 以上である.

32 ビット計算機用の乗算合同法の法が, $2^{31}$ より小さな最大の安全素数 2147483579 である例を考える. 最大周期 $m-1$ の素因数分解は $2 \cdot 1073741789$ である. 最大周期数列から得られる重複しない $t$ 項の組の列の周期は, $t$ が 1073741789 の倍数でない限り, 最大周期の二分の一 1073741789 以上である.

## 2.2 スペクトル検定

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, $\gamma_t$ は, Hermite (エルミート) の定数である).[2]

$T$ 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 [4]. 尺度 $M(T)$ の値は, $(0,1]$ の範囲にあるが, 大きいほうがよい.

## 2.3 系列相関

数列 $\{U_n \mid n \geq 0\}$ の, 遅れ $s$ の系列相関

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

の絶対値が大きい場合, 項 $U_n$ と項 $U_{n+s}$ 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 [5, 第 3.3.3 節].

遅れ 1 の系列相関は効率よく計算されうる: 遅れ 1 の系列相関は, Dedekind 和 $\sigma(a,m)$ を含む式

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

で表される [3, 式 (4.12)]. Dedekind 和 $\sigma(a,m)$ は効率よく計算されうる [3][5].[3]

遅れ $s \geq 2$ の系列相関 $c_s$ は, 遅れ 1 の系列相関を計算する方法によって効率よく計算されうる. なぜなら, 乗数 $a$ に関する遅れ $s$ の系列相関は, 別の乗数 $a^s \bmod m$ に関する遅れ 1 の系列相関に等しいからである.

## 2.4 法の値と乗数の値との選択例と考察

32 ビット計算機で用いられる乗算合同法の法の値と乗数の値とを選定する. 法の値は, $2^{31}$ より小さな最大の安全素数 2147483579 とし, 乗数の値は,

(i) 数列の周期が最大になり (第 2.1.1 節),

(ii) 12 次元までの空間におけるスペクトル検定の結果がよくなり (第 2.2 節),

(iii) 遅れ 1 から遅れ 12 までの系列相関の絶対値が小さくなり (第 2.3 節),

(iv) その乗算合同法が, 効率的なアルゴリズム [9] によって正しく実現される

ように選ぶ. (乗数の値の例を, 発表会で示す.)

# 参考文献


[1] Bratley, P., Fox, B. L., and Schrage, L. E.: *A Guide to Simulation*, 2nd ed., (Springer, New York, 1987).

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

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

[4] 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.

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

[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.

[9] Wichmann, B. A., and Hill, I. D.: "Algorithm AS 183: An efficient and portable pseudo-random number generator," *Applied Statistics* **31** (1982), 188–190; correction, idem **33** (1984), 123.


[2] 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 [2, 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.

[3] Dedekind 和 $\sigma(a,m)$ の定義については, 整数 $c$ の値を零として Knuth [5] による一般 Dedekind 和の定義を参照.