乱数の検定について

奥田英輔

1

モンテカルロ法によるシミュレーションにおいて最も基礎となるのは乱数または擬似乱数である。前者は主として乱数表を引くことにより得られ，後者は電子計算機により「回帰関係による内部的発生」によって得られる。

そこで上のようにして得られる乱数または擬似乱数が望ましい性質をもつか否かを検定することが問題となる。統計学で案出された種々の検定法を適用して行なわれるが，それは乱数の本質とどのような関係があるか。たとえば，１１１……と１ばかり１億個続く数字の列も乱数でないとはいいきれない。10の１億乗分の１の確率があるから。しかし，このような数字の列は統計的検定によって乱数または擬似乱数として不適当だと判定される。

それでは乱数（または擬似乱数）と統計的検定法の間にはどのような関係があるか。

この小論では大数の強法則の観点からこの問題を解明した。

2

フォン・ミーゼスは無限回の試行の列で確率論を組織しようと試みた。これを乱数の基礎づけに適用すると０から９までの10個の数字の無限列がある。そして，どの数字の現われる頻度も等しい極限に収束する。つまり，1/10である。この場合，上の数字の列は乱数となる。

しかし，実際問題として，無限回の試行または数字の列は存在しない。故にフォン・ミーゼスの定義は実際的ではない。

そこで，有限個の数字の列が乱数として適当かどうかを検定することが必要となる。

3

乱数表の作成法とその検定は普通次のように行なわれるようである（1,2,3,4,5,6）。

0から9まで10個の数字を書いたカードをそれぞれ10枚づつ，合計100枚つくる。それら100枚のカードをよくかきまぜて1枚のカードを取り出す。その数字を記録する。そしてカードを元へ戻す。このような操作を何回か行なう。

このようにして得られた数字の列に対して次のような検定を行なう。

(1) 先づ補助乱数表を用意する。それは例えば上のカードの抜き取り操作等によって作られた簡便な乱数表である。主乱数表における0から9までの10個の数字の出現度数を調べる。たとえば，0の出現度数が23個だけ多いならば，補助乱数表を引いて23個の0の数字を他の数字で置きかえる。このようにして各数字の出現度数をおよそ等しくする。

(2) 度数検定：たとえば，相続く50個の数字の列を1組にして，各数字がほぼ同数回出現しているかどうかをしらべる。すなわち各数字の出現回数は等しいという仮説を検定しようというのである。すなわちχ^2一検定を用いる。具体的な計算法については普通の統計学の参考書にのっている。たとえば(7)。

(3) 継次検定：相つぐ2つの数字を組にして考えると，00，01，02，……，99の100通りあるが，これが乱数表でほぼ同数回あらわれねばならない。出現確率がおのおの$\frac{1}{100}$であるという仮説を検定する。χ^2一検定である。

(4) ポーカー検定：相つぐ，たとえば5つの数字をブロックにして考えると，このブロックの数字はすべて異なりａｂｃｄｅの形となることもあれば2つだけが同一で他はすべて異なるａａｂｃｄのような場合等いろいろな場合があるが，もし真の乱数表ならば，これら各種類があらわれる確率は表3・1のようになるので，それを仮説として検定を行なう。

(5) ギャップ検定：乱数列で同じ数字，たとえば0がどれだけの間隔をお

表３・１　ポーカー帰無仮説

型	確率分布
A：a a a a a	0,0001
B：a a a a b	0,0045
C：a a a b b	0,0090
D：a a a b c	0.0720
E：a a b b c	0.1080
F：a a b c d	0.5040
G；a b c d e	0.3024
計	1.0000

表３・２　ギャップ帰無仮説

ギャップの長さ	確率分布	
0	0.1000	
1	0.0900	0.2710
2	0.0810	
3	0.0729	
4	0.0656	0.1975
5	0.0590	
6	0.0531	
7	0.0478	0.1439
8	0.0430	
9	0.0387	
10	0.0349	0.1050
11	0.0314	
12	0.0282	
13	0.0254	
14	0.0228	
15	0.0206	0.2826
16～20	0.0760	
21～25	0.0447	
26以上	0.0646	
和	1.0000	

いて出現するかをしらべる。ギャップの長さは表３・２に示すとおりである。これを帰無仮説として χ^2ー 検定を行なう。こうして比較的不満足なものはすてる。

〔註〕上の検定法は互いに独立ではない。たとえば(1)で数字０の度数が大であれば，(2)で50個の数字の組においても５の出現度数は大であろう。以上５つの検定法は互いに独立ではないようである。

また，どのような検定法を用いるべきかということは全く使用目的によって定まる。そのような検定法を定める普遍的な基準は全く存在しないということを後で示す。

4

擬似乱数の統計的検定法も乱数の場合とほぼ同じである。次に，比較的重要な検定法について述べる（３，８）。

(1)　度数検定：これは３，(1)で述べた０から９までの10個，または，00から99までの 100 個の乱数の度数検定の場合とほぼ同様である。Ｎ個の擬似乱数

r_1, r_2……, r_N の各組に対して，単位区間（0，1）をX個の等しい小区間に分ける。各小区間にはいる乱数の数の期待値はN/xとなる。次に，j＝1，2，……Xに対して，小区間（j－1）/x＜r_i＜j/xにはいる擬似乱数r_i（i＝1，2，……N）の実際の数をf_jとする。すると真の乱数の列に対しては，統計量

$$\chi_1^2 = \left(\frac{x}{N}\right)\sum_{j=1}^{x}\left(f_j - \frac{N}{x}\right)^2 \qquad (4.1)$$

は近似的に自由度 X－1 のカイ二乗分布に従う。この性質で検定を行うな。

(2) 系列検定（9，10）：系列検定は，数列中の相続く数の間の無作為の程度を検査するのに用いられる。系列検定は普通，数の対（2組）に対して適用されるが，この対の擬似乱数は x^2 個の細胞に分割された単位正方形内の点とみなきれる。この考えは3組の場合には単位立方体内の無作為点に拡張される。

はじめに，N個の擬似乱数のM個の連続した組を発生させ，式（4．1）によって擬似乱数のM個の各組に対して，（j－1）/x＜r_i＜j/xおよび（k－1）/x＜r_{i+1}＜k/xを満足する擬似乱数r_i（i＝1，2，……N－1）の数をf_{jk}とする（j，k＝1，2，……，x）。そしてN個の擬似乱数の各組に対して，統計量

$$\chi_2^2 = \frac{x^2}{N-1}\sum_{j=1}^{x}\sum_{k=1}^{x}\left(f_{jk} - \frac{N-1}{x^2}\right)^2 \qquad (4.2)$$

を計算する。しかし，グッド（9，10）は真の乱数列に対しては $\chi_2^2 - \chi_1^2$ が近似的に自由度 $x^2 - x$ のカイ二乗分布に従うことを示している。

(3) 遅延積検定：もう1つ擬似乱数の独立性の度合いを表わすものに遅延積係数がある。kを遅れの長さとするとき，数列r_i（i＝1，2，……，N）に対する遅延積係数 C_k は次のように定義される。

$$C_k = \frac{1}{N-k}\sum_{i=1}^{N-k} r_i r_{i+k} \qquad (4.3)$$

$k>0$ に対して，r_i と r_{i+k} の間の相関がないときは，C_k の値は近似的に平均値 0.25，標準偏差 $1/\sqrt{13N-19k}/12$（$N-k$）の正規分布をすることが示される。正規性の検査にはカイ二乗適度合度検定を応用できる。

(4) 連の検定(8)：擬似乱数の無作為な振動的性格は“連の検定”によって検査することができる。ここでは２つの異なった形式の検定を述べる。すなわち，“上り・下り”の連および“平均値の上側・下側”の連に対する検定である。

上り・下りの連　N個の擬似乱数の列 r_1，r_2，……，r_N に対して，$N-1$ ビットの２進数列Sを次のように定義する。すなわち，Sの第 i 項は $r_i<r_{i+1}$ のとき０に等しく，$r_i>r_{i+1}$ のとき１に等しいとおく。両端が１で区切られたｋ個の０からなる部分列は長さｋの０の連を形成する。１の連についても同様に定義する。検定では，種々の長さの連の実際の発生数を数えて，これらの計数を対応する理論的期待値と比較する。

平均値の上側・下側の連　N個の擬似乱数の列 r_1，r_2，……，r_N に対して，Nビットの２進数列Sを次のように定義する。すなわち，Sの第 i 項は $r_i<1/2$ のとき０に等しく，$r_i>1/2$ のとき１に等しいとおく。

再びSにおける連を数える。長さｋの連の期待数は $(N-k+3)\,2^{-k-1}$，また連の総数の期待値は $(N+1)/2$ となる。カイ二乗検定を用いて，与えられた擬似乱数発生法が受け入れられるかどうかを検査する。

(5) 最大値検定：単位区間（０，１）上のN個の独立な一様乱数の組に対して，確率変数 $R=\max(r_1, r_2, \cdots\cdots, r_N)$ を定義する。この順序統計量により定義される確率分布に対しては，R^N が区間（０，１）上で一様分布をするようになる。R^N の観測値に対する検査には，N個の乱数の数組についてくり返される簡単な度数検定を使う。N個の一様乱数の最大値検定はN組（r_1，r_2，……，r_N）の検定ともいわれるが，これは基本的な度数検定より，いっそう厳しい検定と考えられている。

〔註〕擬似乱数の検定法も乱数の検定法と同様にそれは全く使用目的によって選択されるべきであるが，電子計算機によって発生される擬似乱数の個数は乱数表の乱数の個数よりも著しく多いということである。したがって，この点で乱数の検定法と

は異なった方法を用いなければならないだろうということが当然考えられる。そのことについては次に述べる。

5

電子計算機によるシミュレーションにおいては非常に多くの擬似乱数を必要とする。数十万個とか数百万個の擬似乱数を必要とするシミュレーションは決してまれではない。一様擬似乱数を多数必要とする理由の一つとして一様分布以外の複雑な分布の擬似乱数は一様擬似乱数を複数個用いて合成されるということである。

一様擬似乱数以外の主な擬似乱数について説明すると次の通りである。

正規乱数：（0，1）間の矩形乱数をn個とって，それをV_1，V_2，……，V_Nとする。これらは独立でその平均値は1/2，分数は1/12であるから

$$\frac{V_1+V_2+\cdots\cdots+V_N-(N/2)}{\sqrt{N/12}}$$

は，中心極限定理により，$n\longrightarrow\infty$のとき近似的に標準正規分布N（0，1）にしたがう。標本の大きさは，この場合なら5～10でよいとされている。

自由度nのχ^2分布：正規分布N（0，1）にしたがう，たがいに独立なn個の確率変数の平方和によってえられるから，正規乱数からχ^2乱数がえられる。

指数乱数：自由度2のχ^2分布にしたがう確率数をχ_2^2とおけば，$U=\chi_2^2/2\lambda$は指数分布

$$f(u)\,du=\lambda e^{-\lambda u}du$$

にしたがう確率変数となる。

ポアッソン分布：平均値λのポアッソン分布にしたがう乱数は次のようにして作ることができる。Y_1，Y_2，……はたがいに独立で，指数分布$e^{-u}du$にしたがう確率変数として，順次に

$$Y_1,\ Y_1+Y_2,\ Y_1+Y_2+Y_3,\ \cdots\cdots$$

をつくり，

$$Y_1+Y_2+\cdots\cdots+Y_N\leqq\lambda<Y_1+Y_2+\cdots\cdots+Y_{N+1}$$

を満足するnをもとめると，このnがポアッソン乱数になる。

二項分布 ${}_nC_kP^kg^{n-k}$：区間（0，1）をp：qの長さに分割する。

正規乱数の検定について簡単にのべよう。もと用いた矩形乱数が検定ずみであっても，変換は近似的なものであるから，作られた正規乱数は検定を必要とする。それにはたとえば次のようにする。（i）n個の正規乱数の和またはその平均値は，また正規分布をなすから，x_iを乱数として $t=\Sigma x_i/n$ が正規分布をなすかどうかをみる。(ii) x_i が正規分布をなせば Σx_i^2 は χ^2 分布をなすことに着目して検定する。(iii) その他 range を用いて行なう検定がある。これは正規分布にしたがう確率変数のn個の実現値をとってきた場合，その range（最大値と最小値の差）の分布が理論的にわかっているから，理論的頻度と観察値とを比較することができる。この他，正および負の符号の連なり方の検定，自己相関係数が0になるかどうかをしらべるなどの方法がある。

１１１と１という数字が3個連なって現われる確率は1/1000である。このようなことは数万個の数字から成る乱数表ではきわめてまれなことであろう。故にポーカー検定等でとり除いても，それ程差し支えない。しかし，数十万個，または数百万個からなる擬似乱数列では却って不合理となる。それは１１１を含まない擬似乱数列というのはきわめてまれであるから。実際に確率の非常に小さい事象を問題とするシミュレーションもある (4)。

また，一様乱数以外の乱数を用いるシミュレーションについても上と同様である。そのような場合は，一般的にきわめて多数の確率の小さい一様乱数を必要とする。

故に同じ検定法を用いるにしても，乱数の個数の多少によって適用の仕方が異ならなければならないであろう。さらに異なった検定法を開発する必要もある (4)。

6

擬似乱数は必ず周期性をもつ。これが擬似乱数の最大の弱点である。何故かというと擬似乱数は有限桁の実数であり，それらは有限桁の初期値 x_0 か

らつぎつぎと発生される。

$$x_0 \rightarrow x_1 \rightarrow x_2 \rightarrow \cdots\cdots \rightarrow x_{n-1} \rightarrow x_n \qquad (6.1)$$

たとえば合同法によると，合同式

$$x_N \equiv k x_{N-1} \ (\mathrm{mod} M) \qquad (6.2)$$

によって乱数列を作る。

$$k = 23, \ M = 1.0 + (10)^{-8} \qquad (6.3)$$

この数列は8桁の数字で周期は 5，882，352 である Modulus $= 1.0 + (10)^{-8}$ に対して $k = 23$ の場合がもっともよいことが知られている。それは23より大きい数字をkにとっても周期は長くならないし，23より小さいkの場合には周期は $k = 23$ の場合の周期の半分以上にならないからである。

上の場合，小数8桁までの1.0より小さい実数は $10^8 = 1$ 億個しかない。したがって1億個の擬似乱数を発生させればそれらのうち少なくとも2個は同じものがあるはずである。したがって上の擬似乱数列は周期性をもつ。このことをより一般的に証明しよう。

$$x_{n-1} \longrightarrow x_n \qquad (6.4)$$

なる操作を

$$x_n = f_{m,n}(x_{n-1}) \qquad (6.5)$$

とする。$f_{m,n}$ は関数であるとする。

$f_{m,n}$ は n が変わるにしたがって変わるか，または変わらないかであるとする。つまり変わってもよいし変わらなくてもよい。さらに $f_{m,n}$ は有限個の情報によって規定されているとする。$f_{m,n}$ を規定する情報量のうち最大のものが存在する。すると $f_{m,n}$ は周期性をもつ。擬似乱数の桁数を8とすると $f_{m,n}$ によって作られた擬似乱数列の周期Sは，

$$S \leqq 10^8 X \ (f_{m,n}\text{の周期}) \qquad (6.6)$$

である。（証明了）

擬似乱数 x_0，x_1，$x_2 \cdots$，x_n，… が周期性をもつとすると

$$x = x_0 + 10^{-8} x_1 + 10^{-8\times 2} x_2 + \cdots + 10^{-8\times n} x_n + \cdots$$

は有理数である（循環小数であるから）。逆に有理数を小数点以下8桁づつとって並べるとその数列は周期性をもつ。

無理数であれば周期性をもたない。また，大数の強法則により，殆んどすべての無理小数で0から9までの数字の現われる割合はおのおの10/1である。故に無理数を電子計算機で簡単に計算できればよいがそれは困難でる。たとえば $\sqrt{2}$ を開平により求める計算をみても，桁が進むに従ってそれ以前の情報が累積し計算は非常に困難になる。

検定によって乱数または擬似乱数列

$$x_0, x_1, \cdots, x_n, \cdots \tag{6.7}$$

はパスするか否かである。故に検定は乱数列の有限または無限集合

$$\{(x_0, x_1, x_2, \cdots)\} \tag{6.8}$$

によって表現することができる。前節(5)で述べた検定法では集合（6.8）のすべての元素は有限個の数の組であってよい。故に検定法は有限個の数の組の有限または無限個の集合

$$\{(x_0, x_1, \cdots x_\lambda)\} \tag{6.9}$$

によって表現される。ただし，λは各々の数の組に対して定まっているものとする。

7

フォン・ミーゼスの立場からすれば乱数とは0から9までの10個の数の無限個の列である。また乱数の検定法とは前節(6)で述べたように有限個の数の組がその無限列に含まれているか否かをチェックして，含まれていれば不合格とし，含まれていなければ合格とすることである。

ところが，どのような有限個の数の組もその生ずる確率は必ず零ではない。また大数の強法則によると生起確率が零でない事象はベルヌーイ列には殆んど確実に現われる。故に上述の有限個の数の組は殆んど確実に乱数列に含まれる。

以上をまとめると無限乱数列は殆んど確実に検定をパスしない。これはパラドックスである。ところが，たとえば

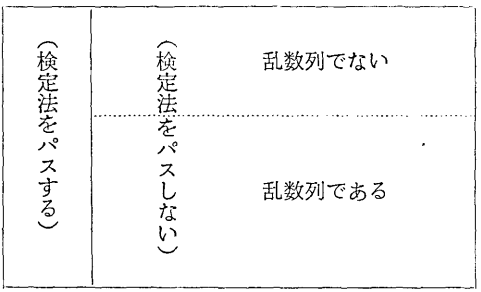
1 1 1 1……

という無限列は検定法はパスしないがフォー・ミーゼスの立場からすると乱

数列でもない。

以上をまとめると7.1図のようになる。

図 7. 1



参 考 文 献

1. Fisher, R. A., and Yates, F. Statistical Tables for Biological Agricultural and Medical Research, London : Oliver and Boyd, 1953.
2. Duparc, H. J. A., Lekkerker, C. G., and Peremans, W. "Reduced Sequences of Integers and Pseudo-Random Numbers," Mathematische Centrum Report ZW 1953—002, Amsterdam (1953).
3. Forsythe, G. E. "Generation and Testing of Random Digits at the National Bureau of Standards, Los Angeles," in Monte Carlo Method. National Bureau of Standards Applid Mathematics Series No. 12. Washington, D. C., 1951.
4. Mize,J. H.,and Cox, J. G. Essentials of Simulatin. Englwood Cliffs. Prentice-Hall, 1962.
5. Good, I. J. "The Serial Test for Sampling Numbers and Other Tests of Randomness" Proc. Camb. Phil. Soc., XLIX (1953), 276—284.
6. Naylor, T. H., Balintfy, J. L., Burdick, D. S., and Chu, K. Computer Simulation Techniques. New York, John Wiley and Sons, 1966.

7. Freund, J. E. Mathematical Statistics. Englewood Cliffs: Pretice-Hall, 1962.
8. International Business Machines Corporation, "Random Number Generation and Testing," Reference Manual (c20—8011), New York, 1959.
9. Coveyou, R. R., "Serial Correlation in the Generation of Pseudo-Random Numbers," Journal of the Association for Computing Machinery, VII (1960), 72—74.
10. Good, I. J. "On the Serial Test for Random Sequences," Annals of Mathematics Statistics XXVIII (1957), 262—264.
11. Green, B. F., Smith, J., and Klem, L. "Empirical Tests of an Additive Random Number Generator," Journal of the Association for Computing Mchinery, VI, No.4 (1959), 527—537.
12. Lehmer, D. H. "Mathematical Methods in Large-Scale Computing Units," Annals Computer Laboratory Harvard University, XXVI (1951), 141—146.
13. Hull, T. E. and Dobell, A. R. "Mixed Congruential Random Number Generators for Binary Machines," Journal of the Ass ociation for Computing Machinary, XI, No. 1 (1964), 31— 40.
14. Greenberger, M., "An a priori Determination of Serial Correlation in Computer Generated Random Numbers," Mathematics of Computations, XV(1961), 383—389.
15. Greenberger, M., "Method in Randomness," Comunications of the ACM, VIII, No. 3 (1965), 177—179.
16. Hull, T. E. and Dobell, A. R. "Random Number Generators," SIAM Review, IV, No.3(Jully 1962) 230—254.