研　究　速　報

UDC 519.28

モンテカルロ法用疑似乱数について

Pseudo-Random Numbers for Monte-Carlo Calculation

岩　本　明　人*
Akito IWAMOTO

1. はじめに

乱数は概念的には容易に理解されるが数字的に定義付けることはむずかしく，かつある決った容量しか持たない計算機内で真の意味を持つ乱数を発生させることは現在では放射線放出等の物理現象を利用しない限り不可能である．しかしこれら物理現象を利用した乱数は，再現しにくく，またその特性を解析しにくい等の困難があり現在ではあまり実用に供されておらずもっぱら計算機内で数式を用いて発生するものが使用されている．この乱数は“真の乱数”と区別して疑似乱数 (Pseudo-random number, 略して PRN) と呼ばれる．この乱数について Lehmer は“各項の配列が当事者以外の人にはわからず，伝統的な統計学の検定およびそれが適用される問題に合った検定に合格した数列についての漠然とした概念”と定義しており，この定義が一般に受け入れられている．

ここではこの PRN の発生法および検定法について述べる．これ等の乱数はすべて〔0, 1〕で一様分布するものであるが，適当な変換を行なえば，任意分布に従う乱数を得ることができる．また実際の FORTRAN によるプログラムも載せて使用者の便を計った．

2. PRN 発生法

計算機を用いた PRN の発生法は現在 i) 初期値を平方し，その平方値の中間のデジットを次の乱数値とする平方採中法 (Mid-square method), ii) 現在公けにされている乱数表を用いる法, iii) 計算機内で数式を用いて乱数を発生させる合同法 (congruential method) が代表的であるが，大量に乱数が必要な時 ii) の方法は不便であり，i) の方法は初期値によっては非常に短い周期を持つ可能性があること，解析しにくい事で現在はもっぱら iii) の方法が用いられている．ここでは，特にその合同法および変形について述べる．

一般に第 n 番目の乱数を R_n とすると合同法は次式で表示できる．

$$R_{n+1}=\alpha R_n+\beta \quad (\mathrm{M\bar{O}D.}\ m) \qquad (1)$$

ここで MŌD はいわゆるモジュラスの計算であり，使用する計算機が γ 進で一語長が P ビットのときは (γ^P-1) を一般には使用している．

また α と β のとる値によって次のように合同法は大別されている．

$\alpha=1,\ \beta=R_{n-1}$　相加型　(2)

$\alpha=$任意，$\beta=0$　乗算型　(3)

$\alpha=\beta=$任意　混合型　(4)

α,β の値について今迄に種々の値が提案されているが，代表的なものを次に列記する．

D型 (乗算型)

$$\left.\begin{aligned}&\alpha=2^{[P/2]}+3\\&\beta=0\\&m=\gamma^P-1\end{aligned}\right\} \qquad (5)$$

〔 〕は Gauss の記号であり，P が35のとき $[P/2]$ は17である．($2^{17}=131072$) この PRN は Moshman が提案したもので理論解析が容易である特長がある．

E型 (混合型)

$$\left.\begin{aligned}&\alpha=2^7+1=129\\&\beta=1\\&m=2^{35}-1\end{aligned}\right\} \qquad (6)$$

F型

$$\left.\begin{aligned}&\alpha=186277,\ 186285,\ 186293,\ 186309,\ 186301\\&\beta=0\\&m=2^{35}-1\end{aligned}\right\} \qquad (7)$$

ここで α が5個あるのはそれぞれの値を乱数的に使用することであり，次に述べるシャッフル型乱数に似ている．

Tien and Moshman[1] が電子管内の電子の振舞をシミュレートしたきに用いた PRN は乗算型の一変形と考えられ，α として 7^{13}(=96889010407) を使用し，乗算によりできた22デジットの内，後半の11デジットを次の乱数として使用している．本文ではこの PRN をA型としている．この PRN は特殊な乱数であり，現在では発生もむずかしくあまり推薦はできない．

次に合同法により作られた2つの PRN 系列を用いて一つの PRN を作るシャッフル型 PRN[3] について述べる．この PRN は乱数性は向上することが期待されるが，発生時間がほぼ2倍位必要であることが欠点といえるが現在のように計算機の演算速度が向上するとこの欠点は無視できる．

シャッフル型乱数は次のように例えば M と N の二

* 元大学院学生，第3部斎藤教授指導

つの乱数系列を使う．ここで仮に M を主乱数列，N をシャッフル乱数列とするとまず計算を続行する前に M 系乱数を 101 個発生させ，始めの 100 個の乱数を計算機の 1 から 100 までの番地の付いたメモリーに表しておく．次に N 系乱数を発生させると使用する乱数はすべて〔0, 1〕で一様であるので 100 倍して整数部分を M 系列乱数表の番地として用い．その番地に格納されている乱数をシャッフル型乱数として使い，後には第 101 番目の M 系の乱数を納入しておく．以下順次この手順を繰り返すことになる．次に具体例を用いて説明する．たとえば図 1 に示すようにすでに乱数表は出来上っている．もし N 系乱数が 0.1732… だとすると，乱数表の第 17 番目の乱数が使用され，その後に第 101 番目の M 系乱数が割り当てられる．次に N 系乱数が，0.2015… であるので乱数表の第 20 番目の乱数が使用され N の項には第 102 番目の乱数が割り当てられることになる．

以上の乱数を分類して表に示す．B, C 型 PRN は本文で述べた D 型 PRN と同様に乗算型である．これ等の PRN に対し初期値は JIS 乱数表によりその値を採用した．ここで注意すべきことは初期値のとり方により式 1 での α, β の値が同じであっても PRN 系列の性質がまったく変ることであり，初期値によっては非常に短かい周期の PRN にしてしまう可能性がある．初期値と一体で PRN は考えるべきである．また，実際に PRN を用いた計算で解析解（もしあれば）と異なった結果を得た場合に PRN を変えてみることも一つの解決手段になりえる．特に，解析解実験解がなく PRN を用いたシミュレーション解のみの場合には PRN を数種使用することは不可欠と思われる．

3. 乱数の検定[2)]

次に乱数の検定について述べる．乱数の検定は一般にその一様性に対する検定であり，頻度，ポーカー，シリアル検定等がある．頻度検定 (Frequency test) はたとえば乱数列の上二桁をとり，それから 1 から 100 迄に一様に分布しているか x^2-検定を行なう方法である．ポーカー検定 (Poker test) は乱数を二進展開して，0 と 1 とがどのような組み合せでどれ位表われるかを検定するものである．

相関の有無を検定する方法[9)] として次の様に表を利用する方法がある．たとえば R_1, R_2, R_3, R_4…… なる乱数列があるとこの数列を (R_1, R_2), (R_3, R_4)…… の如く，(x, y) の組にして x-y 座標にプロットする．組の作り方として (R_2, R_3), (R_4, R_5)…… も同時にプロットする．すると相関の強い乱数列や，短い周期を持つ乱数では直線の集まりとなって表われる．またこの様にしてでき上った小さな図を小さな桝目に区切って，一様性の検定にも使用できる．例を図 2, 3 に示しておく．

また相関を調べる方法として乱数の Fourier 変換[9)]を行なうこともある．すなわち

$$F(n, m)=(RE)^2+(IM)^2 \qquad (8)$$

$$RE=\sum_i \cos 2\pi(nx_i+my_i) \quad n, m: \text{integer}$$

$$IM=\sum_i \sin 2\pi(nx_i+my_i) \qquad (9)$$

x_i と y_i は前述の (x, y) の第 i 番目の組みの値を使う．この方法によると，前述のグラフに直線が表われるとその直線が y 軸に交わる回数の整数倍だけの m の値又は x 軸における m の値に対して強いピークが表われる．この方法を実際の PRN に適用した例を図 3 に示す．

以上述べてきた検定法は一般の一様乱数に対する検定法であるが，その他の検定法として平均値の偏差と任意の乱数の出現頻度を調べることが考えられる．平均値の偏差は乱数列を 100 個づつまとめ，その平均値をもとめたものである．B 型 PRN を使用したその結果を図 4 に示す．グラフは平均値の変動分をとっているので負の値も出て来る．本図よりガウス分布を検定すると 2σ 以内にほとんどの平均値が収まっていることがわかる．

次にある任意の乱数をとり，その乱数がどの位の間隔をあけて現われるかを調べてみた．その結果を図 5 に示す．これ等のグラフは 0 から 9 迄の出現率を平均したものであるが，図 5 には現在信用されている乱数表の一つである Rand 乱数表を調べた結果も同時に示すが，G 型 PRN もほとんど理論曲線に合っており，Rand 乱数表との差を認め難いことがわかる．

図 1

TYPE	GENERATING METHOD	STARTER	REMARKS
A	IR=IR∗7^{13}	96889010407	7^{13}=96889010407 IR is the last 11 digits
B	IR=IR∗19	882195	
C	IR=IR∗5^{11}	989147	5^{11}=48828125
D	IR=IR∗131075	772953	131075=2^{17}+3
E	IR=IR∗129+1	0	129=2^7+1
F	IR=IR∗186211 186285 186293 186309 186301		
G	A shuffled by B	96889010407 882195	
H	D shuffled by E	1253022579 0	

IR is an integer of a pseudo-random number.

図 2

```
      FUNCTION RUNFM (IR, IIR)
      K=INT (RUNFN (ITR)*4.0)+1
      GO TO (1,2,3,4,5), K
    1 IA=186277
      GO TO 6
    2 IA=186285
      GO TO 6
    3 IA=186293
      GO TO 6
    4 IA=186309
      GO TO 6
    5 IA=186301
    6 CONTINUE
      IR=IA*IR
      A=FLOAT (IR)
      RUNFM=AMOD (A, 2147483647.0)/2147483647.0
      RETURN
      END
```

図 3

```
      FUNCTION RUNFN (IIR)
      IIR=IIR*19
      RUNFN=FLOAT (MOD(IIR,2147483647))/2147483547.0
      RETURN
      END
```

図 4

```
      HARP        5020        COMPILED        LIST        RAND
        EXTERNAL FORMULA NUMBER                    SOURCE STATEMENT
      FUNCTION RUNFM (IR)
      DOUBLE LENGTH INTEGER KKL3, KKU, KKU1, KKU2, KKU3
      DOUBLE LENGTH INTEGER IR, IRU1, IRU, IPL, KKL, KKL1, KKL2
      IRU=IR/1000000000
      IRU1=IRU*1000000000
      IRL=IR-IRU1
      KKL=IRL*889010407
      KKL1=KKL/1000000000
      KKL2=KKL1*1000000000
      KKL3=KKL-KKL2
      KKU=IRU*889010407+IRL*96+KKL1
      KKU1=KKU/100
      KKU2=KKU1*100
      KKU3=KKU-KKU2
      IR=KKL3+KKU3*1000000000
      KIR=IR/100
      FKIR=FLOAT (KIR)
      RUNFM=1, OE-9*FKIR
      RETURN
      END
```

図 5

```
      FUNCTION RUNFM (IR, IIR)
      DIMENSION STORE (49), STORE 1 (51)
      DOUBLE LENGTH INTEGER IR
      DATA STORE/
     10.477543,  0.050198,  0.181133,  0.589186,  0.080092,  0.416801,  0.642720,
     20.498424,  0.889548,  0.449984,  0.994042,  0.473562,  0.728628,  0.196785,
     30.780378,  0.243561,  0.884055,  0.552246,  0.683009,  0.889381,  0.906547,
     40.859405,  0.719214,  0.243981,  0.410825,  0.509304,  0.442274,  0.292322,
     50.875608,  0.540983,  0.141468,  0.571365,  0.443617,  0.241480,  0.042076,
     60.570068,  0.721571,  0.745837,  0.505379,  0.129391,  0.580191,  0.637093,
     70.228656,  0.842296,  0.954197,  0.546288,  0.445187,  0.453741,  0.642308/
      DATA STORE1/
     10.752462,  0.124253,  0.260688,  0.107245,  0.782655,  0.171133,  0.512095,
     20.275728,  0.011908,  0.627108,  0.808922,  0.338476,  0.263260,  0.869457,
     30.504131,  0.550210,  0.407751,  0.811461,  0.102680,  0.029649,  0.964421,
     40.102399,  0.661531,  0.559514,  0.700310,  0.327551,  0.189642,  0.386524,
     50.230459,  0.208198,  0.047973,  0.021400,  0.617907,  0.801619,  0.349486,
     60.038862,  0.973694,  0.701094,  0.359139,  0.877629,  0.056860,  0.235904,
     70.893893,  0.640422,  0.874445,  0.671329,  0.722708,  0.893961,  0.281490,
     80.408647,  0.966544/
      MIR=RUNFN (IIR)*100.0+1.0
      IR (MIR. GE. 50) GO TO 1
      RUNFM=STORE (MIR)
      STORE (MIR)=RUNFP (IR)
      RETURN
    1 CONTINUE
      RUNFM=STORE1 (MIR-49)
      STORE1 (MIR-49)=RUNFP (IR)
      RETURN
      END
```

以上の諸検定をここに述べた PRN にあてはめた結果，これ等の PRN は一様でなくはないとの結論を下すことができる．

以上述べた種々の PRN を使用することによりより複雑なより“乱数度”の高い PRN の作製が可能である．それは全てシミュレーションの精度，計算時間に依存する問題である．また PRN の検定は Lehmen の言の如く PRN が摘用される問題に合ったものを使用又は考えるべきである．その他整数理論的な PRN の解析は論文4を参照されたい．

謝　辞

本研究にあたりご指導いただきました本所斎藤教授，藤井助教授に感謝いたします．また統計数理研究所渋谷氏，日立中研島田氏にも種々のご示唆を受けました．あわせて感謝いたします．

(1971 年 4 月 30 日受理)

参 考 文 献

1) P. K. Tien and J. Moshman: “Monte-Carlo Calculation of Noise Near the Potential Minimum of a High Frequency Diode” Jour. Appl. Phys, Vol. 27, No. 9, pp. 1067-1078, Sept. 1957.
2) T. E. Hull and A. R. Dobell: “Random Number Generators” SIAM. Review, Vol. 4, No. 3, pp. 230-254, July 1962.
3) M. D. MacLaren and G. Marsaglia: “Uniform Random Number Generators” JACM, Vol. 12, No. 1, pp. 83-89. Jan. 1965.
4) J. Moshman: “Random Number Generation” Mathematical Methods for digital computers Vol. II, John Willey and Sons pp. 249-263.
5) D. W. Hutchinson: “A New Uniform Pseudorandom Number Generator” CACM, Vol. 9, No. 6, pp. 432-433, June 1966.
6) M. Greenberger: “Method in Randomness” CACM, Vol. 8, No. 3, pp. 177-179, March 1965.
7) A. Rotenberg: “A New Pseudo-random Number Generators” JACM, Vol. 7, No. 1, pp. 75-77, Jan. 1960.
8) R. R. Coveyou: “Serial Correlation in the Generation of Pseudo-random Numbers” JACM, Vol. 7, No. 1, pp. 72-74, Jan. 1960.
9) R. P. Chambers: “Random-Number Generation on Digital Computers” IEEE. Spectrum, pp. 49-56, Feb. 1967.
10) G. Marsaglia, M. D. MacLaren and T. A. Bray: “A Fast Procedure for Generating Normal Random Variables” CACM, Vol. 7, No. 1, pp. 4-10, Jan. 1964.

次 号 予 告 (8月号)