

一様乱数発生ルーチン RANU3

の誤りとその改善法

京大工学部 津田 孝夫

(Takao Tsuda)

京大大型計算機センター乱数発生ルーチン RANU2 は、レーマー型合同法

$$Y_{n+1} = a Y_n + c \quad (\text{mod } m), \quad (1)$$

$$y_n = Y_n / m \quad (2)$$

により一様乱数を発生するもので、標記の RANU3 は RANU2 に shuffle (かきまぜ) の操作を追加して、RANU2 の多次元一様性などに関する欠陥を除くことを意図したものである。しかし 現在提供されている RANU2、RANU3 は両者とも多次元一様性の検定結果は表 1 に示す通り 3 次元以上で不合格である。

表 1 は RANU3 により生成した乱数列 $\{X_n\}$ を規格化して $(0, 1)$ 上の点列 $x_n = X_n/m$ とし、これから r 次元の点列 $(x_0, x_1, \dots, x_{r-1})$, $(x_r, x_{r+1}, \dots, x_{2r-1})$, $\dots$ を単位超立方体の中に落とす。この単位超立方体を各座標軸方向に分割数 p で等分割し、 p^r 個の各小立方体に点の落ちる頻度を χ^2 検定するという常套的な実測である。危険率は 5%, サンプルサイズは 2,000,000。また各小立方体中の理論度数が 10 程度となるよう配慮してある。

RANU3 のアルゴリズムそのものが誤りである。その理由を次に述べる。

[RANU3 による発生 of アルゴリズム]

1. 初期化. URANI (RANU2 の (1) 式と同じもの) により、128 個の乱数 (整数) を発生させ、補助テーブル $T(1), T(2), \dots, T(128)$ に入れる。
2. テーブルのエントリ j の決定. URANI により再び次の乱数 Y を発生し

$$j = Y (\text{mod } 128) + 1 \quad (3)$$

により j をきめる。

3. 乱数の取り出し、おきかえ. $T(j)$ を取り出し、乱数 X とする。 $T(j)$ には j をきめるのに用いた Y を代入。次の新しい乱数 X はステップ 2 にもどれば得られる。

[RANU3 の誤り]

上記補助テーブル $T(1), T(2), \dots, T(128)$ は、 $t = 128 (= 2^7)$ 個の乱数を収納する。一方次の事実が証明できる (岡崎 誠、京大工学部情報工学科特別研究報告、昭和58年2月提出)。付録参照。

“レーマー型合同法 URANI ($a = 2^{15} + 3$ とする)

$$Y_{n+1} = a Y_n + c \pmod{m}, \quad m = 2^{31} \quad (4)$$

により発生される乱数列 $\{Y_n\}$ につき、

$$Y_{n+2^{k-1}} = Y_n \pmod{2^k} \quad (5)$$

が成り立つ。”

RANU3 についていえば

$$Y_{n+2^6} = Y_n \pmod{2^7}$$

であるから、RANU3 により発生される乱数列は、最初の 64 個を除き、以後は RANU2 により発生される乱数列と 全く一致してしまう。RANU3 のインプリメンテーションは誤りで shuffle はきいていない。

[改善法]

t を2のべき乗に選ばない。 $t = 5, 10, 15, 30, 60, 120, 300$ としたときの多次元一様性の表 1 と同様の検定の結果を表 2 に示す。著しい改善があり、 t を 15 または 30 に選ぶだけで十分である。

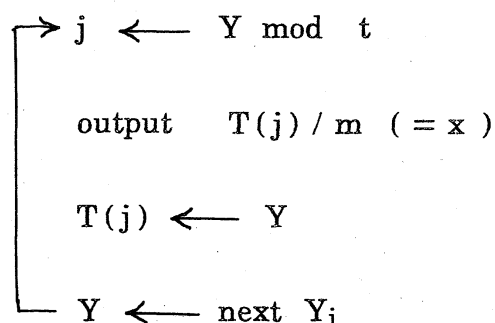
RANU3 はユーザとしては乱数の初期値と発生させる乱数の個数のみしか指定できないようになっているから、早急にルーチンそのものが改善される必要があ

る。

RANU2 そのものも標準ルーチンとして適当でないと思われる。

RANU3 は $Y_i \in \{Y_n\}$ ((4)式)として

$$T(i) \leftarrow Y_i \quad (i=1, 2, \dots, t), \quad Y \leftarrow Y_{t+1}$$

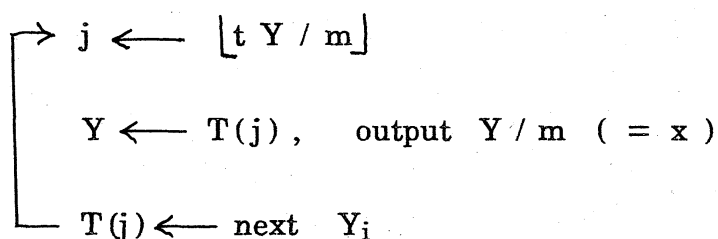


としたもので、 j の決定に乱数 Y_i の下位 β ビット ($2^\beta = t$)を用いる。この β ケタ整数は必ず 2^β の周期をもつ。またmultiplier a の値によっては URANI の場合 ($a = 32771 = 2^{15} + 3$) のようにその下位 β ビットは $2^{\beta-1}$ のより短い周期をもつ。これに対し、上のアルゴリズムの第2行目 $j \leftarrow Y \bmod t$ を $j \leftarrow \lfloor t Y / m \rfloor$ とすることも考えられるが、 t が2のべき乗で $t = 2^\beta$ のとき、これでも j の決定にもとの乱数列 $\{Y_n\}$ の各乱数から直接毎回上位 β ビット切り出して使うことになる。

本来の shuffle 法は次の通りである。

$$T(i) \leftarrow Y_i \quad (i=1, 2, \dots, t)$$

$$Y \leftarrow Y_{t+1}$$



すなわち、 j の決定にもとの乱数列そのままではなく、取り出した乱数(shuffle されている)を使う。

付録。 (5) の証明。

式(1)を変形し、繰り返し用いると

$$Y_n = Y_0 a^n + \frac{c}{a-1} (a^n - 1),$$

$$Y_{n+l} = Y_0 a^{n+l} + \frac{c}{a-1} (a^{n+l} - 1).$$

差をとると

$$Y_{n+l} - Y_n = \frac{(a-1)Y_0 + c}{a-1} a^n (a^l - 1).$$

ここで

$$l = 2^k, \quad (a-1)Y_0 + c = A$$

とおくと

$$\begin{aligned} Y_{n+2^k} - Y_n &= \frac{A a^n}{a-1} (a^{2^k} - 1) \\ &= \frac{A a^n}{a-1} (a^{2^{k-1}} + 1) (a^{2^{k-1}} - 1) \\ &= \frac{A a^n}{a-1} (a^{2^{k-1}} + 1) (a^{2^{k-2}} + 1) (a^{2^{k-2}} - 1) \\ &= \dots \end{aligned}$$

$$\begin{aligned}
&= \frac{A a^n}{a-1} (a^{2^{k-1}} + 1) (a^{2^{k-2}} + 1) \dots \\
&\quad \dots (a^{2^1} + 1) (a^{2^0} + 1) (a^{2^0} - 1) \\
&= A a^n (a^{2^{k-1}} + 1) (a^{2^{k-2}} + 1) \dots \\
&\quad \dots (a^{2^1} + 1) (a^{2^0} + 1)
\end{aligned}$$

(1)において multiplier a は必ず奇数であり、奇数のべき乗は必ず奇数であるので、上式最終右辺のカッコで表される各因数はすべて偶数で少なくともそれぞれ2を1つ因数にもつ。したがって

$$Y_{n+2^k} - Y_n = 0 \pmod{2^k}.$$

さらにRANU3(すなわちURANI)の特殊事情として、 $a = 2^{15} + 3$ としており、 $a+1$ は 2^2 で割り切れる。 $(a+1)$ を除く他の因数は、素因数分解ですべて各1個しか2を含まないことが示せる。従ってRANU3では

$$Y_{n+2^k} - Y_n = 0 \pmod{2^{k+1}}$$

となり、 k を $k-1$ でおきかえれば証明したい(5)が導かれた。

表 1. 京都大学大型計算機センター様乱数ルーチン

RANU2 および RANU3 の多次元一様性

次元数	1次元 当り 分割数	RANU2 χ^2 値	判定	RANU3 χ^2 値	判定	χ^2 臨値 (危険率5%)
1	100	101.82	合	101.87	合	123.30
2	489	232,788.69	合	232,801.19	合	240,255.27
3	62	3,502,404.00	否	3,495,438.00	否	239,460.38
4	22	6,492,937.00	否	6,493,493.00	否	235,378.67
5	11	326,849.81	否	376,841.75	否	161,981.89
8	4	75,231.69	否	74,553.56	否	66,129.86

(1983 年 2 月測定)

表2. 改善したRANU3の多次元一様性

(tは補助テーブルのサイズ)

t = 5

次元数	1次元 当り 分割数	χ^2 値	判定	χ^2 値/閾値
1	100	101.76	合	
2	489	244,134.81	否	1.016
3	62	252,549.87	否	1.055
4	22	251,363.19	否	1.068
5	11	161,320.44	合	0.996
8	4	66,207.87	否	1.001

t = 10

1	100	101.77	合	
2	489	235,186.81	合	0.979
3	62	233,469.81	合	0.975
4	22	235,610.69	否	1.001
5	11	158,783.12	合	0.980
8	4	65,383.91	合	0.989

t = 15

1	100	101.77	合	
2	489	234,092.87	合	0.974
3	62	231,644.75	合	0.967
4	22	230,478.50	合	0.979
5	11	158,421.00	合	0.978
8	4	65,485.28	合	0.990

t = 30

1	100	101.83	合	
2	489	233,464.56	合	0.972
3	62	229,759.44	合	0.959
4	22	230,508.87	合	0.979
5	11	159,322.62	合	0.984
8	4	64,671.15	合	0.978

表2 (つづき)

t = 60

次元数	1次元 当り数 分割数	χ^2 値	判定	χ^2 値/自由度
1	100	101.88	合	
2	489	233,455.31	合	0.972
3	62	229,754.62	合	0.959
4	22	230,246.44	合	0.978
5	11	159,318.69	合	0.984
8	4	65,621.50	合	0.992

t = 120

1	100	101.77	合	
2	489	235,176.56	合	0.979
3	62	230,009.56	合	0.961
4	22	230,796.81	合	0.981
5	11	159,034.00	合	0.981
8	4	65,623.50	合	0.992

t = 300

1	100	102.15	合	
2	489	234,042.06	合	0.974
3	62	230,820.94	合	0.964
4	22	231,217.81	合	0.982
5	11	158,874.81	合	0.981
8	4	65,261.36	合	0.987