数理解析研究所講究録
第537巻 1984年 11-17

乗算合同法の系列相関について

早大　理工　十代田　三知男

Michio Sosiroda

○．はじめに

疑似乱数列の独立性の評価法の一つとして系列相関係数がとりあげられることがある。

本稿は、乗算合同法による乱数列一周期の系列相関係数について、

（1）素数を法とし、その原始根を乗数とする乗算合同法の系列相関係数の高速算法を紹介する。

（2）系列相関係数が比較的小さい　"補数型乗算合同法"を紹介しこの乱数列の系列相関係数の近似式および近似誤差について述べる。

1．素数を法とする乗算合同法の系列相関係数の高速算法

素数を法とする乗算合同法は、

$$x_i = a\,x_{i-1} \mod p \qquad (1)$$

ただし、x_iはi番目の乱数値、pは素数、aはpに関する原始根

で表わされ、任意の初期x_0（$1 \leqq x_0 \leqq p-1$）のとき、周期$T = p-1$で、一周期中に、$1 \leqq x_i \leqq p-1$なる整数をすべて含んでいる。

(1)式による一周期分の数列の系列相関係数$\rho(\tau)$は定義により、

$$\rho(\tau) = \frac{12\sum_{i=1}^{p-1} x_i x_{i+\tau} / p - 3p(p-1)}{(p-1)(p-2)} \qquad (2)$$

ただし、τは"ずらし"の項数（$1 \leqq \tau \leqq p-2$）

で求められる。

いま、(2)式の分子をc_1とすると、

$$c_1 = (p^2 - c_2 p + X_\tau^2 + 1)/X_\tau \qquad (3)$$

ただし、c_2 は不明な整数

X_τ は(1)式において$x_0 = 1$としたときのx_τの値で、

$X_\tau = a \mod p$

で表わせることが試行錯誤により分かった。なお、(3)式中の不明なc_2は(2)式の分子c_1を求めることにより逆算することが出来る。

ここで、(3)式のc_2が分かったものとすると、c_2はさらに

$$c_2 = (X_\tau^2 - c_3 X_\tau + b^2 + 1)/b \qquad (4)$$

ただし、$b = p \mod X_\tau$

のように、(3)式と同じ形で表わせることが分かり、(3)→(4)の操作を続けるとc_iの値は0または3になることを見つけた。

以上の考察よりつぎのような高速算法を得た。

（1）$b_1 \leftarrow p$, $b_2 \leftarrow a^\tau \mod p$

（2）$b_i = b_{i-1} \mod b_{i-2}$なる互乗法を$b_i = 1$になるまで続ける。

（3）$b_i = 1$のとき、$n \leftarrow i$

（4）nが奇数ならば、$c_n \leftarrow 0$

nが偶数ならば、$c_n \leftarrow 3$

（5）$c_{i-1} \leftarrow (b^2_{i-1} - c_i b_{i-1} + b_i^2 + 1)/b_i$

を$i \leftarrow n$から$i \leftarrow i-1$としながらn－1回繰返し、c_1を求める。

（6）素数pを法とする乗算合同法の系列相関係数$\rho(\tau)$は

$$\rho(\tau) = \frac{c_1}{(p-1)(p-2)} \qquad (5)$$

となる。

以上の算法による計算量は、(2)式のO(p)に対しO(logp)となる。

以下に上記算法による数値例を示す。

$p = 41$, $a = 5$ のとき $\tau = 0, 1, 2, 3, \cdots\cdots$ に対する $a^\tau \mod p$ は、(1)式において、$x_0 = 1$ としたときの $x_1, x_2, x_3 \cdots\cdots$ の数列に外ならない。したがって、$\tau = 0, 1, 2, 3, \cdots\cdots$ に対する $a^\tau \mod p$ は

1、5、25、2、10

となる。以下 $\rho(0), \rho(1), \cdots\cdots, \rho(4)$ を順次求める。

$\tau=0$　$5^{0} \bmod 41 = 1$　だから　$b_1=41$, $b_2=1$　で　$n=2$

算法(4)により、nは偶数だから　$c_2=3$

算法(5)により、$c_1=(41^2-3\cdot41+1^2+1)/1=1560$

算法(6)により、$\rho(0)=1560/(40\cdot39)=1$

なお、$\rho(0)=1$は当然であるが、本算法が$\tau=0$でも成立することを示したまでである。

$\tau=1$　$5^{1} \bmod 41 = 5$　だから　$b_1=41$, $b_2=5$, $b_3=1$　で　$n=3$

算法(4)により、nは奇数だから　$c_3=0$

算法(5)により、$c_2=(5^2-0\cdot1+1^2+1)/1=27$

$c_1=(41^2-27\cdot41+5^2+1)/5=120$

算法(6)により、$\rho(1)=120/(40\cdot39)=0.0769$

$\tau=2$　$5^{2} \bmod 41 = 25$　で　$b_1=41$, $b_2=25$, $b_3=16$, $b_4=9$,

$b_5=7$, $b_6=2$, $b_7=1$　で　$n=7$, nは奇数だから　$c_7=0$

算法(5)により、$c_6=(2^2-0\cdot2+1^2+1)/1=6$

$c_5=(7^2-6\cdot7+2^2+1)/2=6$

$c_4=(9^2-6\cdot9+7^2+1)/7=11$

$c_3=(16^2-11\cdot16+9^2+1)/9=18$

$c_2=(25^2-18\cdot25+16^2+1)/16=27$

$c_1=(41^2-27\cdot41+25^2+1)/25=48$

算法(6)により、$\rho(2)=48/(40\cdot39)=0.0307$

$\tau=3$　$b_1=41$, $b_2=2$, $b_3=1$　で　$c_3=0$

算法(5)により、$c_2=(2^2-0\cdot2+1^2+1)/1=6$

$c_1=(41^2-6\cdot41+2^2+1)/2=720$

算法(6)により、$\rho(3)=720/(40\cdot39)=0.4615$

$\tau=4$　$b_1=41$, $b_2=10$, $b_3=1$, $c_2=0$

算法(5)により、$c_2=(10^2-0\cdot10+1^2+1)/1=102$

$c_1=(41^2-102\cdot41+10^2+1)/10=-240$

算法(6)により、$\rho(4)=-240/(40\cdot39)=-0.1538$

つぎに、$p=2^{31}-1$を法とした乗算合同法についての系列相関係数の計算例を示す。

M= 2147483647 A= 16807

T	X(T)	C	LHO(T)
1	16807	274340296114410	0.000059488069
2	282475249	-51929007618	-0.000000011260
3	1622650073	-190443206142	-0.000000041296
4	984943658	61476283470	0.000000013331
5	1144108930	-39048197502	-0.000000008467
6	470211272	23428913838	0.000000005080
7	101027544	-242034916494	-0.000000052483
8	1457850878	-1398060928554	-0.000000303156
9	1458777923	66658269714	0.000000014454
10	2007237709	53586501030	0.000000011620

M= 2147483647 A= 314159629

T	X(T)	C	LHO(T)
1	314159629	54081685830	0.000000011727
2	693984290	-75910599930	-0.000000016460
3	40662312	44550373926	0.000000009660
4	54167458	55616335686	0.000000012060
5	1154642274	-48507548058	-0.000000010518
6	795432399	153370610406	0.000000033257
7	1032446405	621607895934	0.000000134790
8	156834723	-66489757818	-0.000000014418
9	1592186100	-293288582250	-0.000000063597
10	1811979256	15753907446	0.000000003416

M= 2147483647 A= 397204094

T	X(T)	C	LHO(T)
1	397204094	82060325922	0.000000017794
2	2083249653	-91775404434	-0.000000019901
3	858616159	-172780446726	-0.000000037466
4	557054349	142859387310	0.000000030978
5	1979126465	-41350472526	-0.000000008966
6	2081507258	-151619645178	-0.000000032877
7	1166038895	-96376594206	-0.000000020898
8	1141799280	-70237551186	-0.000000015230
9	106931857	20124298194	0.000000004364
10	142950581	-47696074386	-0.000000010342

M= 2147483647 A= 2100005341

T	X(T)	C	LHO(T)
1	2100005341	50022379818	0.000000010847
2	1726177500	-10175258082	-0.000000002206
3	380724663	100783389834	0.000000021854
4	226603865	19858432710	0.000000004306
5	874165784	-41147759046	-0.000000008922
6	1199430051	-383507228250	-0.000000083160
7	2087146631	-42604153806	-0.000000009238
8	1220833483	122330067342	0.000000026526
9	1244895427	-2709654948630	-0.000000587563
10	1402723270	282615510	0.000000000061

2．補数型乗算合同法による系列相関係数

補数型乗算合同法は法を2^sとする一般の乗算合同法に若干手を加えた乱数発生法で、その系列相関係数が一般の乗算合同法のほぼ自乗となることが特徴である。(1)

$$y = a \cdot x_{i-1} \mod m \qquad (6)$$

$$\left.\begin{array}{l} y < m/2 \quad \text{ならば} \quad x_i = y \\ y > m/2 \quad \text{ならば} \quad x_i = m - y \end{array}\right\} \qquad (7)$$

ただし、$m = 2^s$, $a = \pm 3 \mod 8$

補数型乗算合同法は(6),(7)式で表わされ、初期値x_0を任意の奇数としたとき、周期$T = m/4$で、一周期中に $0 < x_i < m/2$ なる奇数をすべて含んでいる。

上記の補数型乗算合同法にける乗数aの選定には系列相関係数の高速算法が必要であるが、その開発が難かしいので、以下にその近似式を示す。

$$\rho(\tau) = \frac{1}{\{\min(X_\tau, X_\tau^{-1})\}^2} - \frac{1}{\{\min(m/2 - X_\tau, m/2 - X_\tau^{-1})\}^2} \qquad (8)$$

ただし、X_τは(6),(7)式において$x_0 = 1$としたときのτ番目のx_τの値

X_τ^{-1}はmを法とするX_τの逆元で、$X_\tau^{-1} > m/2$のときは、

$X_\tau^{-1} \leftarrow m - X_\tau^{-1}$

(8)式による系列相関係数の誤差の絶対値はほとんど1／m以下である。

ただし、$0 < X_\tau < m/2$ の全範囲において、mの大きさに関係なく誤差の絶対値が約0．0044が4箇所、0．0022が4箇所存在する。そのほか、誤差の絶対値が、1／m以上になるものが約2．6％ある。

以上の誤差が大きいと思われるものは、すべて系列相関係数の真値の絶対値の方が近似値の絶対値より大である。

したがって、近似値によって選定された乗数aはそのまま使うことは危険であるので、それらの中から系列相関係数の真値を求めて、さらに選び出す必要があろう。

つぎに、系列相関係数$\rho(\tau)$が相当に小さい補数型乗算合同法の数値例を示す。

（1）十代田、補数型乗算合同法による疑似乱数、数理科学　No.208 ,October 1980

16 M= 65536 A= 1083

T	X(T)	RHO(T)	KINJI	GOSA
1	1083	0.000000932	0.000000850	-0.000000082
2	6759	-0.000000039	0.000000006	0.000000045
3	20035	0.000000020	0.000000043	0.000000024
4	5489	-0.000000069	0.000000113	0.000000182
5	19189	-0.000000067	-0.000000048	0.000000019
6	6775	0.000000057	0.000000020	-0.000000037
7	2707	0.000000122	0.000000124	0.000000002
8	17439	0.000000011	0.000000001	-0.000000010
9	12069	-0.000000226	-0.000000001	0.000000225
10	29063	-0.000000889	-0.000000858	0.000000031

M= 65536 A= 1877

T	X(T)	RHO(T)	KINJI	GOSA
1	1877	0.000000309	0.000000280	-0.000000029
2	15815	-0.000000016	-0.000000101	-0.000000086
3	3053	0.000000031	0.000000155	0.000000123
4	28849	-0.000000069	-0.000000055	0.000000013
5	16837	-0.000000035	-0.000000031	0.000000004
6	14697	-0.000000110	0.000000021	0.000000131
7	4387	0.000000101	0.000000042	-0.000000059
8	23137	0.000000240	-0.000000006	-0.000000246
9	22219	0.000000090	0.000000005	-0.000000085
10	24167	-0.000000002	-0.000000001	0.000000001

M= 65536 A= 3157

T	X(T)	RHO(T)	KINJI	GOSA
1	3157	0.000000010	0.000000047	0.000000038
2	5177	-0.000000652	0.000000015	0.000000667
3	25325	-0.000000020	-0.000000015	0.000000005
4	2895	-0.000000058	0.000000117	0.000000176
5	30011	-0.000000140	-0.000000130	0.000000010
6	20329	0.000000017	-0.000000000	-0.000000017
7	18909	0.000000140	-0.000000006	-0.000000146
8	7583	-0.000000020	0.000000013	0.000000033
9	18891	-0.000000042	-0.000000036	0.000000006
10	1127	0.000000586	0.000000785	0.000000199

M= 65536 A= 3491

T	X(T)	RHO(T)	KINJI	GOSA
1	3491	0.000000066	0.000000005	-0.000000062
2	2615	0.000000210	0.000000144	-0.000000066
3	19461	-0.000000062	-0.000000012	0.000000050
4	22481	0.000000008	-0.000000014	-0.000000022
5	30957	-0.000000359	-0.000000303	0.000000056
6	2023	-0.000000026	0.000000243	0.000000269
7	15595	0.000000018	-0.000000106	-0.000000124
8	18271	-0.000000387	0.000000003	0.000000391
9	17533	0.000000738	-0.000000005	-0.000000743
10	2921	0.000000095	0.000000115	0.000000020

（注）　混合乗算合同法（乗算合同法を含む）により生成された擬似乱数の一周期に渡る自己相関係数は，まずCoveyou，Greenbergerによりその評価が与えられ，次いでJanssonがいくつかの重要な例に対してexactな計算を与えた。　一方，Dieterは独立に混合型乗算合同法による擬似乱数の自己相関係数を計算し，かつユークリッド互除法を用いた高速計算法を与えている。　(2)式の$t=1$の場合はDieterによれば

$$\rho_1 = \frac{12p\ s(a,p)}{(p-2)(p-1)}$$

で与えられ，普通のDedekind和$s(a,p)$の計算に帰着する。aとpとのユークリッドの互除法を行なうDieterの高速計算法は十代田氏の計算法に類似していると思われる。（$\rho(t)$はρ_1の計算に帰着する。）

Coveyou,R.R.: Serial correlation in the generaration of pseudo-random numbers, J. Ass. Comp. Mach. 7,72-74 (1960).

Greenberger,M.: An a priori determination of serial correlation in computer generated random numbers, Math. Comp. 15,383-389(1961).

Jansson,B.: Autocorrelations between pseudo-random numbers, BIT 4,6-27(1964).

Dieter,U. and Ahrens,J.: An exact determination of serial correlations of pseudo-random numbers, Numer. Math. 17,101-123(1971).

Dieter,U.: Pseudo-random numbers: The exact distribution of pairs, Math. Comp. 25,855-883(1971).

（杉原氏：筑波大の指摘と十代田氏の了解の下に，長坂建二がこの注を加えた。）