数理解析研究所講究録
498巻 1983年 199-210

いくつかの合同型一様乱数生成式のスペクトル検定結果について

計量研究所 栗田良春
(Y.KURITA)

§1 はじめに

プログラムというものは，広く使われていればそれだけ慣性が大きい．特に擬似乱数の発生，変換，検定および改善のプログラムはその性格上，致命的な欠陥をもたぬ限り，それを他の"よりよい"と思われるものに取替えるのは困難であるし実現できても時間がかかる．そこでこの分野の研究ではよりよい乱数を作る努力をする一方で，なるべく強力な検定法を援用して現在使われている擬似乱数について組織的にその素姓をあきらかにして，ユーザーに公表することも必要である．

この報告はこの後者の意図に沿ったもので[0,1]一様分布が期待される合同式を用いた乱数の生成法：

$$x_n = a \cdot x_{n-1} + c \mod m \qquad (*)$$

のパラメータ a, m を12組選び6次元までのスペクトル検定および周期全体に亘る系列相関係数 C を求めた結果を示

すものである．　これらのパラメータは本研究集会で話題になったものを主に選んであり．従って一般に流布され使用されている生成式の一部と推測される．

§2　検定項目

前述のように(*)式の乗数aを12種選び，その各々に対して周期Mが 2^{29}，2^{30}，$2^{31}-1$，2^{31}，2^{32} である場合についてTABLE 1.～5. に分けて結果をまとめてある．（たとえば(*)式が乗算型であって $m=2^e$（$e=31$ 又は32）かつ $a \bmod 8 = 3,5$ であれば周期は $m/4$ であるから $M=2^{e-2}$ のTABLEが対応する）．

各表第1列は乗数aの通し番号，第2列がa，第3～7列の上段がそれぞれ2～6次元の超平面構造の汲数 $n_2 \sim n_6$，下段括弧つき数値が"効率の指標としての楕円体の体積"：$\mu_2 \sim \mu_6$ である．

n_i, μ_i；$2 \leq i \leq 6$ について詳しくは文献2) p.p 90～105を参照されたい．n_iはそこでは ν_i と記されており，これは最も粗い超平面群の枚数の目安となるが正確には最大面間隔の逆数である．　参考までに，Fig.1に3次元単位立方体表面近傍の点の配列の様子を示す．これは $M=2^{29}$ のTABLEの第3行（$a=65539$），$n_3=10.86$ に対応する構造

であって，triplet $(x_{3l}, x_{3l+1}, x_{3l+2})$, $l=1,2,\cdots$ による3次元座標のうち立方体表面に $\varepsilon (=1/512)$ 以内の近くにある点だけを展開図の上にプロットしたものである．はさみとのりで立方体を拵えるとその平面群構造がよく判る．

第8列は系列相関係数Cの値を示す．(文献2) pp. 78～87参照)
更に，TABLE 3.については．このM＝$2^{31}-1$が(Mersenne)素数であるので原始根をもちうる．そこで，aがMの原始根であるものについてはaの数値の右肩に◉印を付した．
尚，計算のためのアルゴリズムは文献1)に依る所が多い．

§3 各定数について

これらの検定結果をどのように読むかについては勿論，明確な基準がある訳ではないが文献2)によれば，"$2 \leq t \leq 6$ にたいして μ_t が0.1以上あれば合格，$\mu_t \geq 1$ ならば旗をひるがえしながら合格"とのべられている．この報告では5枚の一覧表の形にまとめてあるので，相互に比較し相対的な評価をすることもできよう．

以下，これら定数の出典を主に記しておく．

1. $16807 = 7^5$．$2^{31}-1$の原始根であって，$m=2^{31}-1$, $c=0$ として IBM S/360 で LLRANDOM の名で呼ばれ

用いられた／ている．$a \ll m$ であるので系列相関係数Cの値は $1/a$ がなりたつ．

2．$32771 = 2^{15} + 3$．Greenberger 提案といわれ，$m = 2^{31}$，$C \neq 0$ として国内で広く用いられている．この検定によれば次の3.と共に最悪の得点である．

3．$65539 = 2^{16} + 3$．$m = 2^{31}$，$C = 0$ としてIBM．RANDU と名付けられ，国内の計算機でも，2.と同様，依然として用いられているのは問題である．

4．$69069 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 23$．文献2) p.105 によればMarsaglia が"最良の乗数の候補"と呼んだものであり，対称形で憶えやすい．$m = 2^{32}$，$C = 0$ として super duper と呼ばれ IBM S/360 で用いられた／ている．各TABLEを見較べると，$m = 2^{32}$，$C \neq 0$ として用いた方がよいようにも思われる．

5．$1664525 = 5^2 \cdot 139 \cdot 479$　文献2)によれば Lavaux 提案とのことであるが詳細は不明である．$2^{31}-1$ の原始根であるが mod 8 = 5 であるから $C = 0$ としても用いることができる．特筆すべきは，$m = 2^{32}$，$C \neq 0$ の場合である．

6．$39894229 = \lfloor 10^8/\sqrt{2\pi} \rfloor + 1$，mod 8 = 5，仁木（統数研）紹介のものである．

7. $48828125 = 5^{11}$, $\underline{\mod 8} = 5$, 小柳(筑波大)提案の国産品.

8. $314159269 = \lfloor \pi \times 10^8 \rfloor + 4$, $\underline{\mod 8} = 5$

文献2) p105.参照.

9. $3972040094 = 2 \cdot 7^2 \cdot 4053103$

西村(慶応大)紹介で. 出典は G.S.Fishman ; JASA 77(377), 1982. pp.129～136. であって $m = 2^{31}-1$, $c = 0$ として用いる.

10, 11. 文献2) p.102 参照.

12. 筆者がかつて, $2^{31}-1$ の原始根をスペクトルテストの節にかけて選び出した乗数のひとつである.[3]

§4. おわりに.

以上, 本研究集会で話題となった合同型生成法を中心に取上げ, スペクトル・テストと系列相関係数の値の2つの観点からの素性を明らかにした. 使用されている他の生成法(合同式法に限らずM系列系その他についても)について更に調査したいと考える. ご存知の方は, 筆者までお知らせ頂ければ大変幸いである:

計量研究所 〒305
茨城県新治郡桜村梅園一丁目1番4号.

文献

1) K nuth,D.E. "THE ART OF COMPUTER PROGRAMMING Vol.2 Seminumerical algorithms" Addison-Wesley 1971

2) 1)の改訂版の和訳：準数値算法／乱数 渋谷政昭訳 サイエンス社 1981.

3) 宮田良春 情報処理 17(9) pp828-834, 23(1) pp100-101.

536870912

	a	n_2	n_3	n_4	n_5	n_6	C
1	0 16807	16807.000	655.764	139.119	46.152	16.912	
		(1.653)	(2.200)	(3.443)	(2.053)	(.225)	.595E-04
2	0 32771	23167.648	10.863	10.770	10.770	10.770	
		(3.141)	(.000)	(.000)	(.001)	(.015)	.271E-04
3	0 65539	23171.891	10.863	10.770	10.770	10.770	
		(3.142)	(.000)	(.000)	(.001)	(.015)	.136E-04
4	0 69069	8142.492	359.908	98.417	43.566	15.556	
		(.388)	(.364)	(.862)	(1.539)	(.136)	.145E-04
5	0 1664525	17621.527	321.260	63.103	34.670	21.307	
		(1.817)	(.259)	(.146)	(.491)	(.901)	.546E-06
6	0 39894229	16854.645	757.885	100.349	56.409	19.235	
		(1.662)	(3.396)	(.932)	(5.600)	(.488)	.489E-07
7	0 48828125	14451.570	225.765	122.041	50.239	29.428	
		(1.222)	(.090)	(2.039)	(3.138)	(6.251)	.442E-06
8	0 314159269	14963.930	308.697	99.167	50.636	22.091	
		(1.310)	(.230)	(.889)	(3.264)	(1.119)	-.293E-07
9	0 397204094	21319.270	772.997	113.868	37.855	23.195	
		(2.660)	(3.604)	(1.545)	(.762)	(1.499)	.124E-05
10	1 566083941	14757.340	594.697	110.390	48.104	18.276	
		(1.274)	(1.641)	(1.365)	(2.525)	(.359)	-.886E-08
11	1 812433253	17424.582	604.743	122.776	51.127	22.045	
		(1.777)	(1.726)	(2.089)	(3.425)	(1.105)	-.502E-07
12	2 100005341	10728.008	744.832	94.837	44.989	18.276	
		(.673)	(3.224)	(.744)	(1.807)	(.359)	.652E-06

ed.830712

TABLE 1. $M = 2^{29}$

1.073741824

	a	n_2	n_3	n_4	n_5	n_6	C
1	0 16807	16807.000 (.826)	655.764 (1.100)	145.829 (2.078)	46.152 (1.026)	16.912 (.113)	.595E-04
2	0 32771	32765.000 (3.141)	10.863 (.000)	10.770 (.000)	10.770 (.001)	10.770 (.008)	.271E-04
3	0 65539	23171.891 (1.571)	10.863 (.000)	10.770 (.000)	10.770 (.001)	10.770 (.008)	.136E-04
4	0 69069	16284.980 (.776)	359.908 (.182)	98.417 (.431)	43.566 (.769)	15.556 (.068)	.145E-04
5	0 1664525	17621.527 (.909)	642.520 (1.035)	63.103 (.073)	53.235 (2.096)	21.307 (.450)	.537E-06
6	0 39894229	16854.645 (.831)	816.356 (2.122)	100.349 (.466)	61.806 (4.421)	19.235 (.244)	.332E-07
7	0 48828125	28903.137 (2.444)	451.531 (.359)	172.864 (4.104)	50.239 (1.569)	30.265 (3.699)	.176E-06
8	0 314159269	29927.863 (2.621)	308.697 (.115)	142.401 (1.890)	50.636 (1.632)	22.091 (.559)	.245E-08
9	0 397204094	30329.676 (2.691)	905.585 (2.897)	138.528 (1.692)	37.855 (.381)	30.100 (3.579)	.125E-05
10	1 566083941	29514.680 (2.549)	857.166 (2.457)	175.812 (4.391)	48.104 (1.263)	18.276 (.179)	-.260E-07
11	1 812433253	17424.582 (.888)	604.743 (.863)	122.809 (1.045)	51.127 (1.713)	29.292 (3.040)	-.139E-07
12	2 100005341	21456.016 (1.347)	744.832 (1.612)	135.196 (1.535)	50.080 (1.544)	28.355 (2.501)	.150E-06

ed.830712

TABLE 2. $M = 2^{30}$

2 147483647

	a	n_2	n_3	n_4	n_5	n_6	C
1	0 16807●	16807.000	638.903	147.248	66.626	29.917	
		(.413)	(.509)	(1.080)	(3.218)	(1.725)	.595E-04
2	0 32771	32771.000	20.905	20.445	20.445	20.445	
		(1.571)	(.000)	(.000)	(.009)	(.176)	.296E-04
3	0 65539	46338.828	9.274	8.718	8.718	8.718	
		(3.141)	(.000)	(.000)	(.000)	(.001)	.131E-04
4	0 69069	32570.262	1078.258	163.129	37.603	27.803	
		(1.552)	(2.445)	(1.627)	(.184)	(1.111)	.145E-04
5	0 1664525●	35247.168	1203.062	163.423	31.337	16.093	
		(1.817)	(3.396)	(1.639)	(.074)	(.042)	.602E-06
6	0 39894229	16945.801	1097.451	174.703	61.855	24.880	
		(.420)	(2.578)	(2.141)	(2.219)	(.571)	.312E-07
7	0 48828125	47108.250	1123.502	100.010	63.143	20.567	
		(3.246)	(2.766)	(.230)	(2.460)	(.182)	.713E-07
8	0 314159269●	37844.855	948.309	192.315	58.541	33.823	
		(2.095)	(1.663)	(3.143)	(1.685)	(3.603)	.198E-07
9	0 397204094●	27705.742	832.431	170.842	69.491	27.568	
		(1.123)	(1.125)	(1.958)	(3.972)	(1.056)	.178E-07
10	1 566083941	26265.941	1299.572	120.391	57.245	27.350	
		(1.009)	(4.281)	(.483)	(1.507)	(1.007)	-.181E-08
11	1 812433253	24305.449	905.646	166.931	59.355	27.037	
		(.864)	(1.449)	(1.784)	(1.806)	(.940)	-.110E-08
12	2 100005341●	43486.977	1201.454	205.653	65.230	31.922	
		(2.767)	(3.383)	(4.110)	(2.895)	(2.546)	.108E-07

ed.830712

TABLE 3. $M = 2^{31} - 1$

2 147483648

	a	n_2	n_3	n_4	n_5	n_6	C
1	0 16807	16807.000 (.413)	655.764 (.550)	186.177 (2.761)	55.893 (1.337)	26.077 (.757)	.595E-04
2	0 32771	32771.000 (1.571)	21.726 (.000)	10.770 (.000)	10.770 (.000)	10.770 (.004)	.297E-04
3	0 65539	46338.121 (3.141)	10.863 (.000)	10.770 (.000)	10.770 (.000)	10.770 (.004)	.136E-04
4	0 69069	32569.961 (1.552)	719.817 (.727)	159.311 (1.480)	59.582 (1.841)	15.556 (.034)	.145E-04
5	0 1664525	35243.055 (1.817)	1285.040 (4.139)	126.206 (.583)	53.235 (1.048)	21.307 (.225)	.544E-06
6	0 39894229	16854.645 (.416)	929.823 (1.568)	100.349 (.233)	73.362 (5.209)	19.235 (.122)	.272E-07
7	0 48828125	46859.707 (3.212)	634.443 (.498)	172.864 (2.052)	54.203 (1.147)	30.265 (1.849)	.119E-06
8	0 314159269	36395.313 (1.938)	308.697 (.057)	142.401 (.945)	56.710 (1.438)	25.534 (.667)	.271E-08
9	0 397204094	30329.676 (1.346)	905.585 (1.449)	169.083 (1.878)	37.855 (.191)	30.100 (1.790)	.313E-06
10	1 566083941	36402.051 (1.939)	857.166 (1.228)	211.901 (4.633)	68.206 (3.618)	25.729 (.698)	.119E-08
11	1 812433253	34849.164 (1.777)	604.743 (.431)	122.809 (.523)	69.757 (4.049)	30.100 (1.790)	-.139E-08
12	2 100005341	42912.027 (2.694)	1180.452 (3.209)	185.413 (2.716)	50.080 (.772)	34.293 (3.914)	.285E-07

TABLE 4. $M = 2^{31}$

4 294967296

	a	n_2	n_3	n_4	n_5	n_6	C
1	0 16807	16807.000 (.207)	1311.527 (2.200)	215.411 (2.474)	55.893 (.669)	26.077 (.378)	.595E-04
2	0 32771	32771.000 (.786)	43.451 (.000)	10.770 (.000)	10.770 (.000)	10.770 (.002)	.303E-04
3	0 65539	65533.000 (3.141)	10.863 (.000)	10.770 (.000)	10.770 (.000)	10.770 (.002)	.136E-04
4	0 69069	65139.926 (3.104)	1439.633 (2.910)	229.791 (3.204)	83.606 (5.006)	15.556 (.017)	.145E-04
5	0 1664525	70277.437 (3.613)	1523.973 (3.452)	252.412 (4.664)	63.969 (1.313)	32.218 (1.346)	.546E-06
6	0 39894229	33709.289 (.831)	1602.459 (4.013)	200.699 (1.864)	73.362 (2.604)	19.235 (.061)	.232E-07
7	0 48828125	46859.707 (1.606)	825.337 (.548)	209.557 (2.216)	67.868 (1.765)	35.043 (2.228)	.489E-07
8	0 314159269	64615.086 (3.054)	617.395 (.230)	142.401 (.472)	56.710 (.719)	37.842 (3.533)	.312E-08
9	0 397204094	60659.352 (2.691)	967.302 (.883)	169.083 (.939)	75.710 (3.049)	30.100 (.895)	.787E-07
10	1 566083941	68262.375 (3.408)	1442.078 (2.925)	211.901 (2.317)	68.206 (1.809)	25.729 (.349)	.111E-07
11	1 812433253	65779.438 (3.165)	1209.486 (1.726)	122.809 (.261)	69.757 (2.024)	30.100 (.895)	-.696E-09
12	2 100005341	50827.629 (1.890)	1341.983 (2.357)	228.862 (3.152)	67.646 (1.736)	34.293 (1.957)	.958E-08

ed.830712

TABLE 5. $M = 2^{32}$

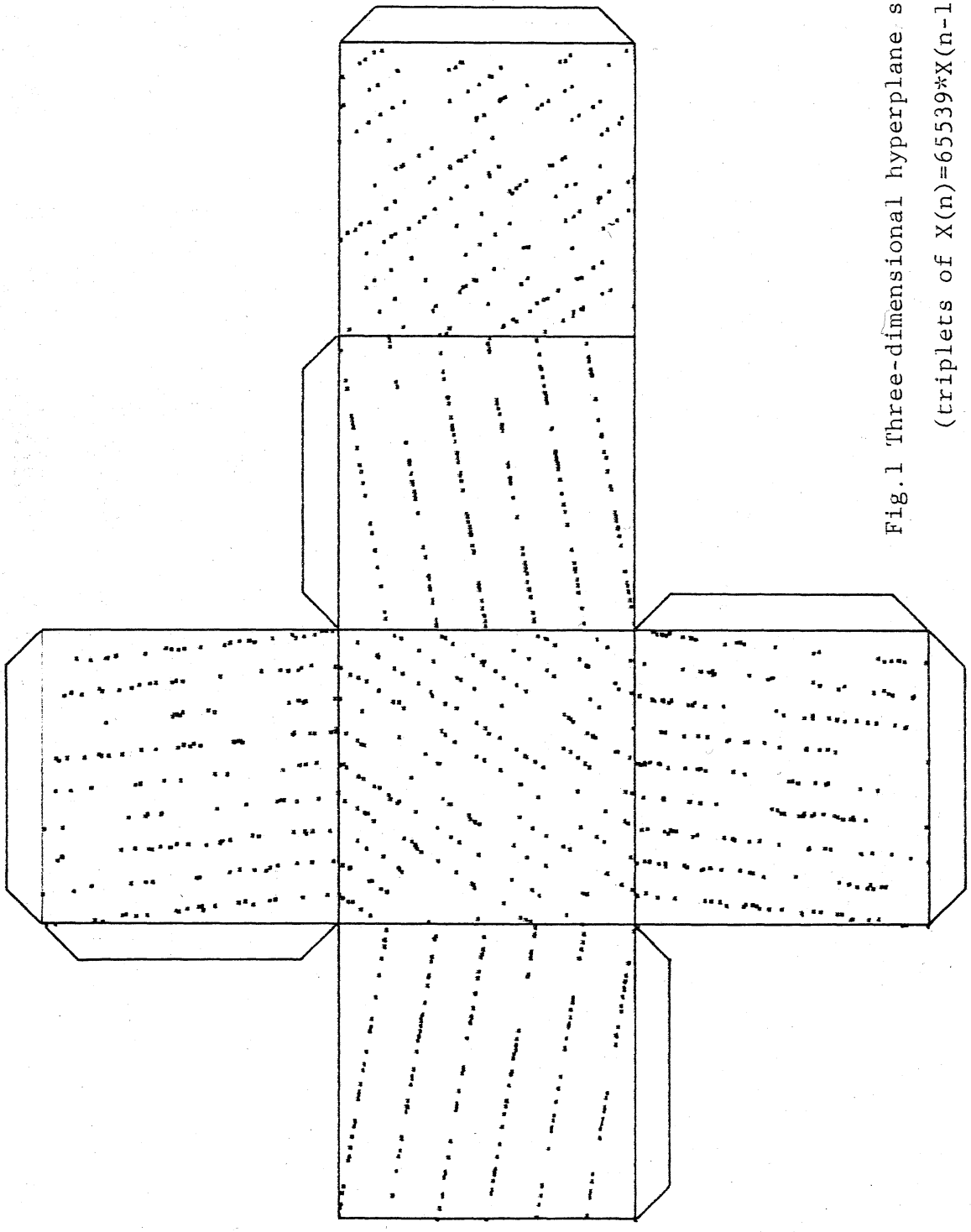

Fig.1 Three-dimensional hyperplane structure.
(triplets of X(n)=65539*X(n-1) mod 2**31)