Printed from:

Robustness of Statistical Methods and Nonparametric Statistics

Edited by
Dieter Rasch and Moti Lal Tiku



VEB Deutscher Verlag der Wissenschaften Berlin 1984

Results of Comparisons Between Different Random Number Generators

FEIGE, K.-D.; GUIARD, V.; HERRENDÖRFER, G.; HOFFMANN, J.; NEUMANN, P.; PETERS, H.; RASCH, D.; VETTERMANN, Th.

Stall from various research establishments in the GDR have investigated generators of equidistributed pseudorandom numbers in regard of their statistical properties. The tests were performed on the following computers:

ES 1040 by Ms. Peters (Rostock)
BESM-6 by Dr. Neumann (Dresden)
CDC-1604 A by Mr. Vettermann (Bohlitz-Ehrenberg)
KRS 4200 by Dr. Feige (Dummerstorf-Rostock).

Apart from investigating several multiplicative generators of the type

$x_{n+1} = (a\ x_n)\ \mathrm{mod}\ M$

and generators of the mixed type

$x_{n+1} = (a\ x_n + b)\ \mathrm{mod}\ M$

(fixed point arithmetic in some cases but floating point arithmetic others), the group also studies a few special techniques for generating random numbers.

The parameters of the generators are given in table 1.

In case 4a) the algorithm certainly seems quite complicated, but in fact it represents merely a bit shift generator: Bits 16 and 32 of a 32-place binary number are combined in such a way that they yield a new bit information which is then attached to the preceding random number. The possible overflow at the beginning of the random number is ignored. When programmed in an assembler language, generators of this type are usually very fast.

Thumhart's generator consists of four multiplicative components that are combined in such a manner that, by means of a special transformation, the index for the next generator is calculated from the preceding random number.

Following up an idea expressed by McLaren and Prof. Marsaglia in 1965, Mr. Teuscher found in 1979 new parameter combinations for a random number generator which in practical terms consists of two independent, hierarchically arranged multiplicative generators. The generator works on the principle that 128 random numbers are first calculated with the first generator. The second generator is then used to select random numbers pseudorandomly from the 128 numbers and to replace each selected number by the next one calculated by the first generator.

Most generators were programmed in the assembler language of the computer concerned, although FORTRAN was used in some cases (only FORTRAN was used for the BESM-6).

With each generator 10 000 random numbers (RN) were generated, the same 10 starting points (x_0) being used in each case. The generators were subjected to the following tests by using these random numbers:

G - χ^2-test for equi-distribution in 100 equidistant classes in (0,1),

R - χ^2-test for the two-dimensional distribution of consecutive pairs of numbers (lag 1, 2, 3 and 4) in 10 X 10 classes,

I - χ^2-interval test in respect of omission of a certain interval $I_i \subseteq (0,1)$, (I_i: (0,

0.2), I_2: (0.2, 0.4),.. I_5: (0,8, 1)),

M - χ^2-maximum test for evaluating the distribution that might be expected on the assumption of the equidistribution of the generator,

$\bar{x}$, s^2 - the mean, variance, skewness and kurtosis of the RN sequence was • put as an
γ_1, γ_2 additional, descriptive from of generator evaluation,

- some members of the group ascertained the number of ascending or descending sequences (v_1, v_2) of RN and the number of RN above or below the arithmetic mean (n_0) of a sample of 10000 RN. n_1, or n_2 are the numbers of sequences below or above the arithmetic mean of the sample.

The different results are presented in tables 2-5. If you find in the tables an A, then initial test shows that the properties of this particular generator are bad.

We propose that the following best generators be used in the subroutine versions we have elaborated for the different computers:

CDC-1604 A

$$x_{n+1} = (5^{15} x_n + 1) \bmod 2^{35} \quad \hat{=}\ (2e)$$

ES 1040

$$x_{n+1} = \left(10^{14} \pi x_n + 10^{14} \sqrt{3}\right) \bmod 10^{14} e \quad \hat{=}\ (2f)$$

$$x_{n+1} = (5^{13} x_n) \bmod 2^{39} \quad \hat{=}\ (1f)$$

$$x_{n+1} = (7^{13} x_n) \bmod 2^{31} \quad \hat{=}\ (5h)$$

and with good results

$$x_{n+1} = (2^{10} x_n) \bmod 1049399 \quad \hat{=}\ (4c)$$

$$y_{n+1} = (8323\, y_n) \bmod 2^{28}$$

KRS 4200

$$x_{n+1} = (2^{10} x_n) \bmod 1049399 \quad \hat{=}\ (4c)$$

$$y_{n+1} = (8323\, y_n) \bmod 2^{28}$$

BSM-6

$$x_{n+1} = (3141592221\, x_n + 1) \bmod 2^{35} \quad \hat{=}\ (2b)$$

$$x_{n+1} = (5^{17} x_n) \bmod 2^{42} \quad \hat{=}\ (1e)$$

While testing the uniformly distributed random number generators, the group at Dummerstorf also analysed the properties of transformers which, at least approximately, transform the random numbers of a (0,1)-equidistribution into a normal distribution.

We tested the following transformations:

a) $$u_n = \sqrt{\frac{\pi}{8}} \ln \frac{1 + x_n}{1 - x_n}$$

b) $$|u_n| = \frac{2.30753 + 0.27061\, z_n}{1 + 0.99229\, z_n^2} - z_n$$

with

$$z_n = \sqrt{-2 \ln x_n} \qquad x_n < 0.5$$

$$z_n = \sqrt{-2 \ln (1 - x_n)} \qquad x_n \geq 0.5$$

c) $$u_1 = x_1 \sqrt{\frac{-2 \ln z}{z}}$$

$$u_2 = x_2 \sqrt{\frac{-2 \ln z}{z}}$$

with

$$z = x_1^2 + x_2^2 \text{ and } 0 < z < 1$$

d) $$u_1 = \sqrt{-2 \ln x_1} \cos 2\pi x_2$$

$$u_2 = \sqrt{-2 \ln x_1} \sin 2\pi x_2$$

e) $$|u_n| = z_n + \frac{\left(((z_n \cdot p_4 + p_3) z_n + p_2) z_n + p_1\right) z_n + p_0}{\left(((z_n \cdot q_4 + q_3) z_n + q_2) z_n + q_1\right) z_n + q_0}$$

with

$$z_n = \sqrt{-2 \ln x_n} \qquad \text{for } x_n < 0.5$$

and

$$z_n = \sqrt{-2 \ln (1 - x_n)} \qquad \text{for } x_n \geq 0.5$$

$p_0 = -0.322232431088$	$q_0 = 0.99348462606 \cdot 10^{-1}$
$p_1 = -1.$	$q_1 = 0.588581570495$
$p_2 = -0{,}342242088547$	$q_2 = 0.531103462366$
$p_3 = -0.0204231210245$	$q_3 = 0.10353775285$
$p_4 = -0.453642210148 \cdot 10^{-4}$	$q_4 = 0.385607006341 \cdot 10^{-2}$

The class limits for the χ^2-test were selected so that the same expected frequencies E_i can be assumed for the 25 classes on the condition of an N(0,1)-normal distribution. In the table 6 we have included a couple of selected observed frequences. The χ^2-test of fit, finally, also permits only the second and fifth transformation to be performed on the KRS 4200 and on the ES 1040 again.

Table 1

Generators

1. Multiplicative Generators

$x_{n+1} = (a\, x_n) \bmod M$

	a	M
a)	82027	2^{32}
b)	$2^{13} + 6$	$2^{23} + 1$
c)	$5 + 8^6$	2^{35}
d)	5^{15}	2^{35}
e)	5^{17}	2^{42}
f)	5^{13}	2^{39}
g)	65539	2^{31}

2. Generators of mixed typ

$x_{n+1} = ((a\, x_n) + b) \bmod M$

	a	b	M
a)	$2^{10} + 1$	101	2^{36}
b)	3141592221	1	2^{35}
c)	2718281821	1	2^{35}
d)	5^{13}	1	2^{35}
e)	5^{15}	1	2^{35}
f)	$10^{14}\,\pi$	$10^{14}\,\sqrt{3}$	$10^{14}\,e$

3. Mixed generators (floating point arithmetic)

	a	b	M
a)	e	$\sqrt{3}$	10.
b)	e	0.	1.
c)	e	$\sqrt{3}$	1.

4. Special techniques

a) $x_{n+1} = 2x_n \bmod 2^{32} + \left(\left(\frac{x_n}{2^{31}} + \frac{x_n}{2^{16}} \bmod 2\right) + 1\right) \bmod 2$

b) Thumhart's generator (Roe (1970))

4 multiplicative generators with

$a_1 = 252\,114\,903\,917$

$a_2 = 8\,064\,131\,757$

$a_3 = 282\,629$

$a_4 = 4\,357$

$M = 2^{35}$

the index I_n for the next generator is calculated with

$$I_n = \frac{\left(a_{I_n} x_n\right) \bmod 2^{38} - \left(a_{I_n} x_n\right) \bmod 2^{36}}{2^{36}}$$

c) McLaren — Marsaglia (1965)
(special parameters Teuscher (1979))

$$x_{n+1} = 2^{10}\, x_n \bmod 1049339$$

$$y_n + 1 = 8323\, y_n \bmod 2^{38}$$

$$I_{n+1} = y_{n+1} / 2^{21} \Rightarrow 7 \text{ bit}$$

5. Additional generators
(only tested on ES 1040 computer)

a) $x_{n+1} = 10^7 x_n \bmod 10006499$

(but other starting points)

b) $x_{n+1} = \left(10^{14}\pi x_n + 10^{14}\sqrt{3}\right) \bmod 10^{14} e$

(and then like 4c) — gen.)

c) $x_{n+1} = 5x_n$

if $x_{n+1} > A \Rightarrow x_{n+1} = x_n - A$

$x_{n+1} > B \Rightarrow x_{n+1} = x_n - B$

$x_{n+1} > C \Rightarrow x_{n+1} = x_n - C$

else $x_{n+1} = x_n$

with A = 137 438 953 472
B = 68 719 476 736
C = 34 359 738 368
and x_0 = 11 919 641 733

	a	b	M
d)	97	788 675	100 001
e)	3^{26}	—	10^{13}
f)	7^5	—	$2^{31} - 1$
g)	7^9	—	$2^{31} - 1$
h)	7^{13}	—	$2^{31} - 1$
i)	3^{17}	—	10^{10}
j)	3^{19}	—	10^{10}
k)	10 006 499	—	$2^{31} - 1$

Table 2
Results for CDC-1604 A

Gen.	G	R	I	M
1a)	95.5	87.7— 105.8	5.5— 7.9	79.8—102.1 (*)
1b)	99.7	85.8— 98.4	7.5— 9.9	29.5— 38.6 (*)
1c)	96.1	85.3— 106.7	6.5—11.8	83.2— 90.8 (*)
1d)	96.5	96.3— 110.8 (*)	6.1— 7.5	83.0— 96.9
1e)	104.6	97.0— 104.0 (*)	7.9— 9.8	90.6—112.0 (*)
1f)	98.1	85.3— 102.5	5.9—11.0	64.4— 95.3 (*)
2a)	89.9	92.0— 109.8	7.3— 9.1	86.2— 99.9 (*)
2b)	89.9	94.0— 104.1	5.7—10.3	66.3— 88.4 (*)
2c)	100.8	94.5— 103.2	7.3—10.7 (*)	60.8— 85.1
2d)	95.8	92.8— 102.4	5.3— 9.9	84.3— 87.5 (*)
2e)	88.7	86.1— 97.6	5.6— 9.2	66.5— 82.3
3a)	105.5	94.5— 119.9	7.8—11.2 (*)	85.0— 90.0 (*)
4a)	101.9 (*)	968.9—40045. (*)	1353.0 (*)	500000 (*)
4b)	102.8 (*)	92.6— 108.0 (*)	6.2— 8.3	70.8— 85.5
4c)	101.4	97.8— 108.8 (*)	6.6—10.6	48.9— 94.4
theor. values	124.3	124.3	16.9	124.4

Table 2
(continuation)

Gen.	u_1	u_2	$\bar{x}$	s^2	γ_1	γ_2
1a)	—	—	—	—	—	—
1b)	—	—	—	—	—	—
1c)	—0.07	—0.25	0.5014	0.0835	—0.0039	—1.2070
1d)	—0.76	—0.22	0.4988	0.0835	0.0003	—1.1994
1e)	0.76	0.15	0.4992	0.0826	—0.0004	—1.1905
1f)	0.17	0.27	0.5003	0.0831	0.0003	—1.1962
2a)	—	—	—	—	—	—
2b)	0.24	1.05	0.4999	0.0829	0.0044	—1.1981
2c)	0.18	0.60	0.4990	0.0834	0.0044	—1.1981
2d)	—0.21	—0.12	0.4982	0.0827	0.0099	—1.1923
2e)	0.31	—0.27	0.5003	0.0829	0.0002	—1.1975
3a)	—0.08	0.63	0.4970	0.0838	0.0120	—1.2065
4a)	—	—	—	—	—	—
4b)	—	—	—	—	—	—
4c)	—	—	—	—	—	—
theor. values	± 1.96	± 1.96	0.5000	0.0833	0.0	—1.2

Table 3
Results for ES 1040

Gen.	G	R	I	M	n_0	$v_1 \approx v_2$
1a)	118.1	131.1	14.3	159.1	4975—5034	3291—3369
1b)	112.3	144.1	17.6	383.9	4974—5050	3282—3351
1c)	123.0	116.0	24.9	218.4	4983—5023	3301—3355
1d)	150.8	127.6	18.3	140.1	4949—5045	3305—3375
1e)	116.9	136.5	22.6	2244.1	4975—5031	3300—3350
1f)	115.7	124.6	17.8	108.1	4959—5046	3303—3364
2a)	128.5	124.2	19.3	129.2	4918—5005	3264—3340
2b)	155.3	127.8	20.4	149.0	4922—5021	3281—3364
2c)	144.5	138.0	19.0	170.0	4904—5071	3286—3388
2d)	108.4	134.4	19.8	246.4	4945—5028	3289—3350
2e)	114.3	121.4	28.5	642.6	4978—5032	3306—3385
2f)	133.4	112.3	16.0	119.0	4971—5073	3290—3370
4c)	102.4	135.0	17.2	130.0	4966—5044	3289—3373
5a)	115.26	110.9	23.0	126.0	4947—5050	3294—3353
5b)	112.6	116.8	17.4	257.0	4949—5043	3303—3364
5c)	122.3	10121.0	19.7	24540.0	4953—5063	2982—3047
5d)	115.2	115.7	22.4	183.9	4960—5063	3309—3362
5e)	112.2	126.0	19.6	117.2	4952—5012	3302—3355
5f)	114.0	117.6	15.4	171.8	4961—5067	3293—3361
5g)	123.9	127.5	13.5	415.3	4951—5028	3293—3369
5h)	128.5	150.5	19.2	113.1	4966—5028	3313—3377
5i)	127.5	115.6	15.7	127.0	4915—5049	3285—3359
5k)	130.3	115.8	16.4	179.5	4963—5045	3302—3381
5l)	120.8	144.1	19.8	103.1	4949—5049	3284—3372
theor. values	123.2	123.2	15.5	123.2	5000	3333

Table 3
(continuation)

Gen.	$n_1 \approx n_2$	x	s^2	γ_1	γ_2
1a)	2454—2535	0.5004	0.0828	—0.0248	—1.211
1b)	2427—2540	0.4985	0.0833	0.0277	—1.172
1c)	2465—2528	0.4975	0.0835	0.0331	—1.232
1d)	2450—2551	0.5006	0.0840	—0.0245	—1.217
1e	2447—2539	0.4998	0.0831	0.0248	—1.218
1f	2465—2530	0.5005	0.0833	—0.0298	—1.170
2a)	2447—2528	0.4970	0.0828	0.0443	—1.178
2b)	2474—2548	0.4987	0.0838	0.0421	—1.215
2c)	2454—2539	0.5009	0.0824	0.0409	—1.160
2d)	2455—2508	0.5003	0.0832	0.0198	—1.171
2e)	2464—2528	0.5001	0.0837	—0.0230	—1.225
2f)	2461—2514	0.4992	0.0838	—0.0267	—1.224
4c)	2469—2531	0.5004	0.0834	—0.0329	—1.181
5a)	2438—2533	0.4999	0.0832	—0.0278	—1.230
5b)	2469—2528	0.4997	0.0833	0.0833	—1.170
5c)	1973—2080	0.5009	0.0836	—0.0306	—1.232
5d)	2428—2531	0.5004	0.0829	—0.0325	—1.182
5e)	2473—2543	0.5000	0.0834	—0.0834	—1.214
5f)	2444—2523	0.5005	0.0831	—0.0344	—1.176
5g)	2473—2551	0.4995	0.0828	—0.0189	—1.166
5h)	2455—2520	0.5008	0.0835	—0.0179	—1.213
5i)	2475—2527	0.4983	0.0834	0.0372	—1.213
5k)	2472—2528	0.4995	0.0834	0.0351	—1.229
5l)	2443—2532	0.4999	0.0832	0.0363	—1.174
theor. values	2500	0.5	0.0833	0.0	—1.2

Table 4
Results for BESM-6

Gen.	G	R	I	M	$\bar{x}$	s^2	γ_1	γ_2
1c)	122.4	125.6	22.2	299.1	0.4970—0.5049	0.0824—0.0846	—0.0268	—1.23
1d)	120.6	143.0	15.0	262.1	0.4952—0.5028	0.0821—0.0842	0.0300	—1.17
1e	111.2	132.3	14.2	517.5	0.4980—0.5036	0.0826—0.0847	0.0144	—1.18
1f)	122.1	116.1	22.5	227.7	0.4958—0.5049	0.0830—0.0850	—0.0310	—1.23
2b)	107.1	119.0	16.9	174.8	0.4964—0.5046	0.0818—0.0838	—0.0229	—1.18
2c)	134.6	130.2	19.2	118.9	0.4943—0.5033	0.0823—0.0846	—0.0235	—1.18
2d)	116.1	144.4	16.8	235.9	0.4943—0.5018	0.0818—0.0834	0.0318	—1.18
3a)	131.9	142.3	31.8	115.9	0.4933—0.5048	0.0816—0.0833	—0.0274	—1.17
theor. values	123.2	123.2	15.5	123.2	0.5000	0.0833	0.0	—1.2

Table 5
Results for KRS 4200

Gen.	G	R	I	M	x	s^2
1a)	2064—2346	209.0—294.1	1.96—26.1	160.3—401.6	0.483—0.489	0.083—0.0852
1b)	106.3—174.3	101.6—259.4	7.6—16.2	35.7—114.0	0.498—0.503	0.083—0.0835
1c)	98.1—127.2	79.3—2611.5	9.5—117.1	100.9—546.6	0.498—0.507	0.0822—0.0835
1d)—1f)	A	A	A	A	A	A
1g)	493.1—512.3	1082—35839	A	A	0.544—0.557	0.0786—0.082
2a)	53147	25879—50107	2687	388.4—547.3	0.340—0.3411	0.1051—0.1061
2b)—2e)	A	A	A	A	A	A
3a)	210.8—269.7	23560	225.3—828.1	255—17342.5	A	A
3b)	246.4—344.3	527—82473	315.1—1014.9	500—193020	0.460—0.474	0.0769—0.0777
3c)	553.7—728.1	1078—24707	23.9—866.3	259.5—1245.0	0.498—0.503	0.0926—0.0951
4a)	A	A	A	A	A	A
4b)	34689	27245—31652	756.4—1761.9	3039.5—3356.2	0.308—0.310	0.0986—0.098
4c)	72.6—109.1	78.8—124.0	4.1—17.1	45.5—94.1	0.496—0.503	0.0823—0.0842
theor. values	123.2	123.2	15.5	123.2	0.5000	0.08333

Table 6
Results of the comparison of N(0,1)-transformations

transf.	intervals							
	(—2.054)	(2.054,1.751)	(1.751,1.555) min.	...	(0.1509,0.107) max.	(0.107—0.0502)	(0.0502—0.)	χ^2-value	time
a	7200	4262	3680	,	3991	3997	4000	2900.4	1.00
b	4006	3992	3980	,	4032	4036	4045	2.25	1.95
c	4066	4015	3945	,	4014	3974	4247	18.2	2.20
d	3848	3841	3942	,	3981	4250	4507	80.6	2.85
e	3918	4034	3998	,	4009	4000	3999	2.1	3.15
E_i	4000	4000	4000		4000	4000	4000		

in all cases N = 100 000

References

Mac LAREN, M. D., MARSAGLIA, G., BRAY, I. A.: A fast procedure generating exponential random variables. Communications of the ACM 7 (1964) 5, 298-300

TEUSCHER, F.: Ein hierarchischer Pseudo-Zufallszahlengenerator. Unveröffentlichte Praktikumsarbeit, Dummerstorf (1979)