Statistische Hefte 27, 315–326 (1986)

Statistische Hefte
Statistical Papers

Algorithms

A non-linear congruential pseudo random number generator

Jürgen Eichenauer and Jürgen Lehn

Received: September 17, 1986; Revised version: November 27, 1986

A non-linear congruential pseudo random number generator is introduced. This generator does not have the lattice structure in the distribution of tuples of consecutive pseudo random numbers which appears in the case of linear congruential generators. A theorem on the period length of sequences produced by this type of generators is proved. This theorem justifies an algorithm to determine the period length. Finally a simulation problem is described where a linear congruential generator produces completely useless results whereas good results are obtained if a non-linear congruential generator of about the same period length is applied.

1. Introduction

The most common method of generating pseudo random numbers to be used for simulations is the linear recursive congruential method. The generators have the form

$$(1) \qquad x_{n+1} \equiv a \cdot x_n + b \pmod{m}, \quad 0 \leq x_{n+1} < m, \quad n \geq 0,$$

where m is a (large) positive integer and x_0, a and b are non-negative integers less than m. This type of generators goes back to Lehmer (1951) and Rotenberg (1960). It is well known (see e.g. Afflerbach 1983, Beyer 1972, Beyer et.al. 1971, Coveyou 1969, Dieter 1979, Knuth 1981, Marsaglia 1968, 1970, and 1972, Schmitz and Lehmann 1985) that the vectors of

AMS 1980 subject classification
Primary: 65 C 10 Secondary: 68 J 99

Key words and phrases
pseudo random number generator, lattice structure, period length

d consecutive pseudo random numbers of the sequence $(x_n/m)_{n\geq 0}$ form a lattice in the d-dimensional unit cube $[0,1]^d$ and that the d-dimensional volume of an unit cell of this lattice is $1/m$ if the generator (1) has maximal period length m.

These generators have the advantage that the lattice structure admits a theoretical analysis of the generated sequences. A lot of work has been done in this direction by many authors and numerical methods to determine generators with a "good" lattice structure have been developed (see e.g. Afflerbach 1983, Afflerbach and Grothe 1985, Beyer 1972, Beyer et.al. 1971, Dieter 1975 and 1979. Marsaglia (1968) however regards this property as a defect caused by the linearity of (1) "that cannot be removed by adjusting the starting value, multiplier, or modulus" (see Marsaglia 1968, p. 25). So the analysis of non-linear generators suggest itself. Knuth (1981, p. 25) e.g. proposed the quadratic congruential pseudo random number generator

$$x_{n+1} \equiv a \cdot x_n^2 + b \cdot x_n + c \pmod{m}, \quad 0 \leq x_{n+1} < m, \quad n \geq 0,$$

where m is a (large) positive integer and x_0, a, b and c are non-negative integers less than m. Knuth (1981, p. 34) gave necessary and sufficient conditions for the maximal period length m to be attained. These conditions show that for $a \not\equiv 0 \pmod{m}$ the maximal period length m can be reached only if m is not a prime number. In this case however the vectors of consecutive pseudo random numbers form a superimposition of shifted lattices (see Eichenauer and Lehn 1986).

In this paper the non-linear congruential pseudo random number generator

$$(2) \qquad x_{n+1} \equiv \begin{cases} a \cdot x_n^{-1} + b \pmod{p}, & x_n \neq 0 \\ b, & x_n = 0 \end{cases}, \quad 0 \leq x_{n+1} < p, \quad n \geq 0$$

is analyzed, where p is a prime number, a and b are positive integers, x_0 is a non-negative integer less than p, and x^{-1} denotes the uniquely determined positive integer less than p with $x \cdot x^{-1} \equiv 1 \pmod{p}$, i.e. the inverse of x in $GF(p)$. To avoid trivial cases $p \geq 5$ is assumed. This generator does not have the property that lattices or superimpositions of lattices are produced.

A fast method of determining the inverse x^{-1} based on the Euclidean al-

gorithm is described in Aigner (1975, p. 48):

1. Let $z_{n+2} = p$, $z_{n+1} = x$ and determine a monotone decreasing sequence of positive integers $z_n, \ldots, z_2$, $z_1 = 1$ with $z_i = z_{i+2} - q_{i+1} \cdot z_{i+1}$, $1 \leq i \leq n$.
2. Let $w_1 = 1$, $w_2 = 0$ and $w_i = q_{i-1} \cdot w_{i-1} + w_{i-2}$, $3 \leq i \leq n+2$. Then $x^{-1} = (-1)^{n+1} \cdot w_{n+2}$ holds.

This algorithm requires an average of about $n \cong 12 \cdot \ln 2/\pi^2 \cdot \ln p$ steps (see Knuth 1981, p. 357). The calculation of a pseudo random number by the non-linear generator (2) therefore needs an average of about $12 \cdot \ln 2/\pi^2 \cdot \ln p + 1$ times more time than the generation of a pseudo random number by the linear congruential generator (1). This factor is approximately 12,6 (18,5) for $p \cong 10^6$ (10^9).

It is clear that the non-linear congruential generator (2) should only be used if one has any reason to avoid lattices. On the other hand in many simulation problems a lot of calculations have to be performed besides the pseudo random number generation so that the time needed to generate a pseudo random number often can be neglected. In this connection it should be mentioned that division modulo p can be implemented in hardware almost as fast as ordinary division as Knuth (1986) pointed out.

2. The period length of the non-linear congruential generator

The sequence $(x_n)_{n \geq 0}$ generated by the non-linear congruential generator (2) consists of at most p different numbers. Therefore $x_s = x_t$ holds for some $t > s \geq 0$. Since x_{n+1} and

$$x_{n-1} \equiv \begin{cases} a \cdot (x_n - b)^{-1}, & x_n \not\equiv b \\ 0, & x_n = b \end{cases}, \quad 0 \leq x_{n-1} < p$$

are determined uniquely by x_n the sequence is purely periodic, i.e. $x_n = x_{n+r}$ holds for $r = t-s$ and every $n \geq 0$. The integer

$$\lambda(p,a,b; x_0) = \min \{k \geq 1 \mid x_0 = x_k\}$$

is called the period length of a non-linear congruential generator (2).

Let $\pi_o(x_o) = 1$ and for $n \geq 1$

$$\pi_n(x_o) \equiv x_o \cdot \ldots \cdot x_{n-1} \pmod{p}, \quad 0 \leq \pi_n(x_o) < p.$$

Since $x_1 = b$ for $x_o = 0$

$$\pi_n(b) \equiv x_1 \cdot \ldots \cdot x_n \pmod{p}.$$

Therefore the period length of a sequence with $x_o = 0$ is given by

$$\lambda(p,a,b;\, 0) = \min \{n \geq 1 \mid \pi_n(b) = 0\}. \tag{3}$$

Lemma 1: Let the sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ be generated by (2) for some x_o and $y_o = b$. Assume $x_o,\ldots,x_{l-2}$, $y_1,\ldots,y_{l-3} \geq 1$ for some $l \geq 2$. Then

$$\pi_n(x_o) \equiv a \cdot \pi_{n-2}(b) + x_o \cdot \pi_{n-1}(b) \pmod{p}$$

for $2 \leq n \leq l$.

Proof: For $2 \leq n \leq l$

$$\pi_n(x_o) \equiv \pi_{n-1}(x_o) \cdot (a \cdot x_{n-2}^{-1} + b) \equiv a \cdot \pi_{n-2}(x_o) + b \cdot \pi_{n-1}(x_o) \pmod{p} \tag{4}$$

follows from (2). Since

$$\pi_2(x_o) \equiv x_o \cdot (a \cdot x_o^{-1} + b) \equiv a \cdot \pi_o(b) + x_o \cdot \pi_1(b) \pmod{p}$$

and for $l \geq 3$

$$\begin{aligned} \pi_3(x_o) &\equiv x_o \cdot x_1 \cdot (a \cdot x_1^{-1} + b) \equiv x_o \cdot a + x_o \cdot (a \cdot x_o^{-1} + b) \cdot b \\ &\equiv a \cdot \pi_1(b) + x_o \cdot \pi_2(b) \pmod{p} \end{aligned}$$

the assertion is valid for $n = 2$ and $n = 3$. Using (4) by induction for $l \geq 4$

$$\begin{aligned} \pi_n(x_o) &\equiv a \cdot \pi_{n-2}(x_o) + b \cdot \pi_{n-1}(x_o) \\ &\equiv a \cdot (a \cdot \pi_{n-4}(b) + x_o \cdot \pi_{n-3}(b)) + b \cdot (a \cdot \pi_{n-3}(b) + x_o \cdot \pi_{n-2}(b)) \\ &\equiv a \cdot \pi_{n-2}(b) + x_o \cdot \pi_{n-1}(b) \pmod{p} \end{aligned}$$

follows for $4 \leq n \leq l$. □

By (2) $x_o = x_1$ is equivalent to $x_o \equiv a \cdot x_o^{-1} + b \pmod p$, i.e. $4 \cdot (x_o^2 - b \cdot x_o - a) \equiv (2 \cdot x_o - b)^2 - (4a + b^2) \equiv 0 \pmod p$. This gives a condition for the existence of starting values x_o which are reproduced by the generator (2). Recall r is a quadratic residue modulo p if there is an integer q with $r \equiv q^2 \pmod p$.

Lemma 2: There exists a starting value x_o with $x_o \equiv a \cdot x_o^{-1} + b \pmod p$ if and only if $4 \cdot a + b^2$ is a quadratic residue modulo p. If $4 \cdot a + b^2 \equiv 0 \pmod p$ then x_o is uniquely determined modulo p; otherwise there exist exactly two different non-negative starting values x_o and $\bar{x}_o$ less than p such that

$$x_o \equiv a \cdot x_o^{-1} + b \pmod p \quad \text{and} \quad \bar{x}_o \equiv a \cdot \bar{x}_o^{-1} + b \pmod p$$

respectively.

Lemma 3: Let the sequence $(x_n)_{n \geq 0}$ be generated by (2). Assume $x_o \neq x_1$ and $x_n \geq 1$ for all $n \geq 0$. Then $\lambda(p,a,b; x_o) = \lambda(p,a,b; 0) + 1$.

Proof: By Lemma 1 it follows that

$$\begin{aligned} & x_o \cdot \pi_n(x_o) - \pi_{n+1}(x_o) \\ & \equiv x_o \cdot (a \cdot \pi_{n-2}(b) + x_o \cdot \pi_{n-1}(b)) - (a \cdot \pi_{n-1}(b) + x_o \cdot \pi_n(b)) \\ & \equiv (x_o^2 - a) \cdot \pi_{n-1}(b) + x_o \cdot a \cdot \pi_{n-2}(b) - x_o \cdot (a \cdot \pi_{n-2}(b) + b \cdot \pi_{n-1}(b)) \\ & \equiv (x_o^2 - bx_o - a) \cdot \pi_{n-1}(b) \pmod p \end{aligned}$$

for every $n \geq 1$. The assumption $x_o \neq x_1$ gives $x_o^2 - bx_o - a \not\equiv 0 \pmod p$. Therefore

$$\lambda(p,a,b; x_o) = \min \{n \geq 1 \mid x_o = x_n\}$$

$$= \min \{n \geq 1 \mid x_o \cdot \pi_n(x_o) \equiv \pi_{n+1}(x_o) \pmod p\} = \min \{n \geq 1 \mid \pi_{n-1}(b) = 0\}$$

and (3) prove the lemma. □

The main result on the period length is the following

Theorem: Let a, b, and p be the parameters of a non-linear congruential generator (2).

(i) $\lambda(p,a,b;\,0) + 1$ divides $p-1$ if $4a+b^2 \not\equiv 0 \pmod p$ is a quadratic residue modulo p.

(ii) $\lambda(p,a,b;\,0) = p-1$ if $4a+b^2 \equiv 0 \pmod p$.

(iii) $\lambda(p,a,b;\,0) + 1$ divides $p+1$ if $4a+b^2$ is not a quadratic residue modulo p.

Proof: By Lemma 2 it follows from the assumption in (i) that there exist exactly two different non-negative starting values x_o' and x_o'' less than p such that each of them is reproduced by the generator (2). Therefore the set $\{0,1,\ldots,p-1\} \setminus \{x_o',x_o''\}$ has $\lambda(p,a,b;0)$ elements or is according to Lemma 3 a union of disjoint sets, one of which with $\lambda(p,a,b;0)$ elements and each of the others with $\lambda(p,a,b;\,x_o)$ elements, i.e. there exists an integer $t \geq 0$ such that

$$\lambda(p,a,b;\,0) + t \cdot \lambda(p,a,b;\,x_o) = p-2.$$

In the case that $t > 0$ the starting value x_o satisfies the assumption of Lemma 3.

Therefore a second application of this lemma gives

$$(t+1)(\lambda(p,a,b;0) + 1) = p-1$$

by which (i) is proved.

The existence of an integer $t \geq 0$ with

$$(t+1)(\lambda(p,a,b;0) + 1) = p$$

follows by the same considerations as in (i). Since p is a prime number this proves (ii).

By Lemma 2 it follows from the assumption in (iii) that there exists no starting value which is reproduced by (2). Therefore the set $\{0,1,\ldots,p-1\}$ has $\lambda(p,a,b;0)$ elements or is according to Lemma 3 a union of disjoint sets, one of which with $\lambda(p,a,b;0)$ elements and each of the others with $\lambda(p,a,b;0) + 1$ elements, i.e. there exists an integer $t \geq 0$ such that

$$\lambda(p,a,b;0) + t \cdot (\lambda(p,a,b;0) + 1) = p$$

by which (iii) is proved. □

3. An algorithm to determine the period length

Let a, b and p be as in (2) and define the sequence $(\tau_n)_{n\geq 0}$ by

$$\tau_n \equiv b \cdot \tau_{n-1} + a \cdot \tau_{n-2} \pmod{p}, \quad 0 \leq \tau_n < p, \quad n \geq 2, \tag{5}$$
$$(\tau_1, \tau_0) = (1,0).$$

Lemma 1 shows $\tau_{n+1} = \pi_n(b)$ for $0 \leq n \leq \pi\ \lambda(p,a,b;0)$ and (3) gives

$$\lambda(p,a,b;0) = \min \{n \geq 1 \mid \tau_n = 0\} - 1.$$

It is known (see e.g. Knuth 1981, p. 28) that for every prime number p there exist positive integers a and b less that p such that the sequence $(\tau_n)_{n\geq 0}$ defined by (5) has period length $p^2 - 1$.

For such a sequence $\min \{n \geq 0 \mid (\tau_{n+1}, \tau_n) = \lambda \cdot (1,0),\ 1 \leq \lambda < p\} = p+1$. Thus $\lambda(p,a,b;0) = \min \{n \geq 1 \mid \tau_n = 0\} - 1 = p$. This shows the existence of non-linear congruential generators (2) with maximal period length p for every prime number p. By the matrix $A = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}$ the recursion (5) can be written in the form

$$\begin{pmatrix} \tau_n \\ \tau_{n-1} \end{pmatrix} \equiv A^{n-1} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{p}, \quad 0 \leq \tau_n < p, \quad n \geq 2.$$

Now the theorem in section 2 justifies the following algorithm for determining the period length $\lambda(p,a,b;0)$ of some given non-linear congruential generator (2) with parameters a, b and p. Therefore a generator with maximal period length p for some given prime number p can be found by applying the algorithm to different parameters a and b (with fixed p) until the calculation ends up with $\lambda(p,a,b;0) = p$.

Algorithm:

1. If $4 \cdot a + b^2 \not\equiv 0 \pmod{p}$ then 3.
2. Set $\lambda(p,a,b;0) = p-1$. End.
3. If $4 \cdot a + b^2$ is a quadratic residue modulo p then 5.
4. Determine the divisors $t_1 < \ldots < t_r$ of $p+1$ being greater than 2. Let $i = 0$ and go to 6.
5. Determine the divisors $t_1 < \ldots < t_r$ of $p-1$ being greater than 2. Let $i = 0$.
6. Let $i = i+1$ and calculate the matrix

$B = (b_{jk})_{1\le j,k\le 2} \equiv A^{(t_i-1)} \pmod p$. If $b_{11} \not\equiv 0 \pmod p$ then 6.

7. Set $\lambda(p,a,b;0) = t_i - 1$. End.

4. Remarks

1. A lot of empirical tests (frequency tests, serial tests, runs up and down tests) have been applied to sequences generated by many different non-linear congruential generators (2) with maximal period length. The modulus p has been chosen near 10^6. The results of these empirical tests give no reason to dissuade one from using a non-linear congruential generator (2) to generate a sequence of pseudo random numbers.

2. To enlarge the period length without extending the time needed for the calculation of one pseudo random number one may combine such generators in the following way: Let $p_1,\dots,p_k$ denote different prime numbers for some $k \ge 2$. Let $(x_n^{(i)})_{n\ge 0}$, $1 \le i \le k$, be the sequence of numbers generated by a non-linear congruential generator (2) with modulus p_i and maximal period length p_i. Define the sequence $(z_n)_{n\ge 0}$ of pseudo random numbers by

$$z_{j\cdot k+i-1} = x_j^{(i)}/p_i \in [0,1)$$

for $1 \le i \le k$ and $j \ge 0$.

This sequence has period length $q = p_1 \cdot \dots \cdot p_k$, i.e.
$q = \min\{r \ge 1 \mid z_{r+n} = z_n \text{ for every } n \ge 0\}$.

3. In the introduction of this paper it was remarked that Marsaglia (1968) regarded the lattice structure as a defect of the linear congruential generator (1). The following example shows that there are in fact simulation problems where completely useless results are obtained if linear congruential generators (1) are applied thoughtlessly whereas good results are achieved if non-linear congruential generators (2) of about the same period length come into use. Of course, one cannot recommend the application of non-linear congruential generators (2) instead of linear congruential generators (1) in general. But they should be applied if one has the feeling that there is something wrong with the

simulation results and one suspects that this is caused by the lattice structure of the linear congruential generator.

Example: If one is interested in the distribution of the minimal distance of two different out of $k \geq 2$ points which are randomly chosen in the unit square, one may calculate an approximation of the distribution function F_k of the random variable

$$M_k = \min \{|X_i - X_j| : 1 \leq i < j \leq k\}$$

where $X_1, \ldots, X_k$ are independent two-dimensional random variables uniformly distributed on the unit square. Since for small $t > 0$ the geometrical probabilities are approximately

$$P(M_2 > t) \cong 1 - \pi t^2$$

$$P(M_{k+1} > 1) \cong (1 - k\pi t^2) \cdot P(M_k > t), \quad k \geq 2,$$

it follows that

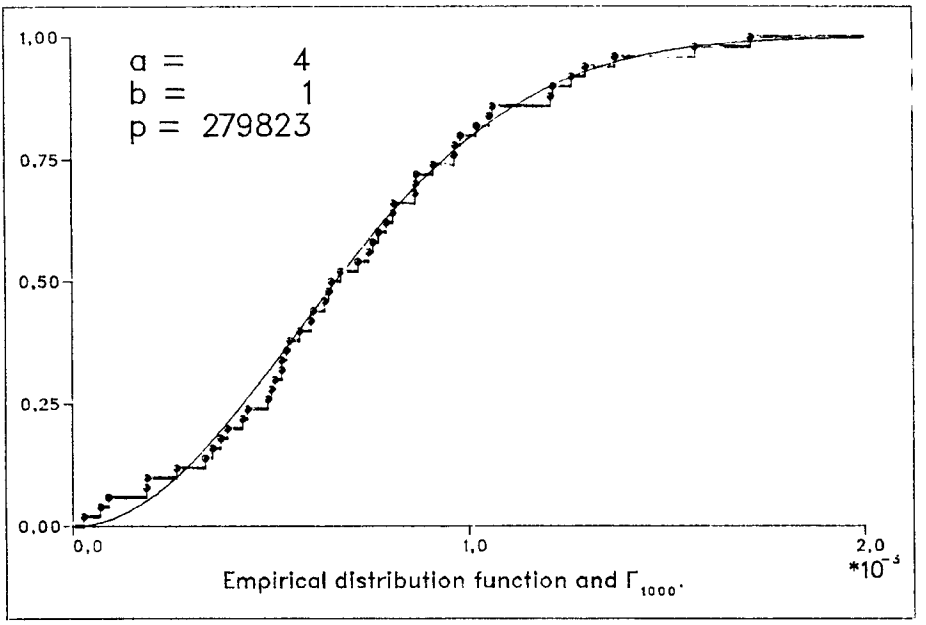
$$F_k(t) \cong 1 - \prod_{i=1}^{k-1} (1 - i\pi t^2) = 1 - \exp\Big(\sum_{i=1}^{k-1} \ln(1 - i\pi t^2)\Big)$$

$$\cong 1 - \exp\Big(-(\pi t^2 \sum_{i=1}^{k-1} i + \frac{1}{2}\pi^2 t^4 \sum_{i=1}^{k-1} i^2)\Big)$$

$$= 1 - \exp\Big(-\frac{1}{2} k(k-1)\pi t^2 \,(1 + \frac{1}{6}(2k-1)\pi t^2)\Big).$$

One may also carry out simulations in order to obtain an approximation of the distribution function. Using thereby for $k = 1000$ the linear congruential generator (1) with $a = 7200$, $b = 1$ and $m = 279\,841$ which is a good one compared with other linear congruential generators of about the same period length, almost all simulations produce the value 0.001993 which is the length of the shortest lattice vector $(-272/m, 487/m)$ in the two-dimensional lattice generated by the linear congruential generator (see e.g. Dieter 1975, p. 831, for a method to calculate this vector). One cannot obtain smaller values than 0.001993 by using this generator although according to the approximation given above the probability of smaller values is greater than 0.99. On the other hand the non-linear congruential generator (2) of about the same period length with $a = 4$, $b = 1$ and

p = 279823 produces results which are consistent with the distribution function F_{1000}, at least if they are compared with the approximation given above.



4. The following table contains the parameters a and p of non-linear congruential generators (2). If b = 1 then each of these generators has maximal period length p. The sequences generated by these generators have been analyzed with the help of empirical tests. For every prime number p and every positive integer e less than p the non-linear congruential generator (2) with parameters $\tilde{a} \equiv e^2 \cdot a \pmod{p}$, $1 \leq \tilde{a} < p$, and $\tilde{b} = e$ where the value of a is taken from the table has maximal period length p, too.

p	999 953	999 959	999 961	999 979	999 983
a	3	5	19	4	11
p	1000 003	1000 033	1000 037	1000 039	1000 081
a	1	5	18	4	21

Acknowledgements: The authors would like to express their gratitude to Professor Knuth for the hints given in a personal communication. They also wish to thank Mr. Rettig for his programming assistance and the Deutsche Forschungsgemeinschaft for financial support.

References

Afflerbach, L. (1983) Lineare Kongruenz-Generatoren zur Erzeugung von Pseudo-Zufallszahlen und ihre Gitterstruktur. Dissertation, TH Darmstadt

Afflerbach, L. and Grothe, H. (1985) Calculation of Minkowski-reduced lattice bases. Computing 35, 269-276

Aigner, A. (1975) Zahlentheorie. deGruyter, Berlin - New York

Beyer, W.A. (1972) Lattice structure and reduced bases of random vectors generated by linear recurrences. In: S.R. Zaremba (Ed.) Applications of number theory to numerical analysis, 361-370

Beyer, W.A.; Roof, R.B. and Williamson, D. (1971) The lattice structure of multiplicative pseudo-random vectors. Math. Comp. 25, 345-363

Coveyou, R.R. (1969) Random number generation is too important to be left to chance. Studies in applied mathematics, SIAM III, 70-111

Dieter, U. (1975) How to calculate shortest vectors in a lattice. Math. Comp. 29, 827-833

Dieter, U. (1979) Schwierigkeiten bei der Erzeugung gleichverteilter Zufallszahlen. Proc. in Oper. Res. 8, 249-272

Eichenauer, J. and Lehn, J. (1986) On the structure of quadratic congruential sequences, Technische Hochschule Darmstadt, Fachbereich Mathematik, Preprint Nr. 1000

Knuth, D.E. (1981) The art of computer programming, vol. 2, 2nd ed., Addison-Wesley

Knuth, D.E. (1986) Personal communication

Lehmer, D.E. (1951) Mathematical methods in large-scale computing units. Ann. Comp. Lab., Harvard Univ. 26, 141-146

Marsaglia, G. (1968) Random numbers fall mainly in the planes. Proc. Nat. Acad. Sci. 61, 25-28

Marsaglia, G. (1970) Regularities in congruential random number generators. Numer. Math. 16, 8-10

Marsaglia, G. (1972) The structure of linear congruential sequences. In: S.K. Zaremba (Ed.) Applications of number theory to numerical analysis, 249-285

Rotenberg, A. (1960) A new pseudo-random number generator. Journ. ACM 7, 75-77

Schmitz, N. and Lehmann, F. (1985) Monte-Carlo-Methoden I, 3rd. ed., Skripten zur Mathematischen Statistik Nr. 2, Universität Münster

Jürgen Eichenauer
Jürgen Lehn
Fachbereich Mathematik
der Technischen Hochschule Darmstadt
Arbeitsgruppe Stochastik und Operations Research
Schloßgartenstr. 7
6100 Darmstadt