MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 184
OCTOBER 1988, PAGES 757–759

A Nonlinear Congruential Pseudorandom Number Generator with Power of Two Modulus

By Jürgen Eichenauer, Jürgen Lehn, and Alev Topuzoğlu

Abstract. A nonlinear congruential pseudorandom number generator is studied where the modulus is a power of two. Investigation of this generator was suggested by Knuth [7]. A simple necessary and sufficient condition is given for this generator to have the maximal period length.

1. Introduction and Notation. The most frequently used pseudorandom number generators are the linear recursive congruential generators. It is well known (see, e.g., Beyer et al. [1] and Knuth [6]) that the vectors of d consecutive pseudorandom numbers form a sublattice of the d-dimensional full integer lattice. Marsaglia [8] regards this lattice structure as a defect of these generators, and in Eichenauer and Lehn [2] a simulation problem is described which supports Marsaglia's view.

Therefore, nonlinear congruential pseudorandom number generators are introduced and studied (see, e.g., Eichenauer and Lehn [2], [3], Eichenauer et al. [4], [5] and Knuth [6, p. 25]). In particular, the nonlinear generator

$$(1) \qquad x_{n+1} \equiv \begin{cases} a \cdot x_n^{-1} + b \pmod{p}, & x_n \geq 1, \\ b, & x_n = 0, \end{cases} \qquad x_{n+1} \in \mathbf{Z}_p,\ n \geq 0,$$

is analyzed in Eichenauer and Lehn [2], where p is a prime number, $x_0 \in \mathbf{Z}_p = \{0, 1, \ldots, p-1\}$, $a, b \in \mathbf{Z}_p \backslash \{0\}$, and x_n^{-1} denotes the inverse element of x_n in the Galois field $\mathrm{GF}(p)$. In this paper the nonlinear generator

$$(2) \qquad x_{n+1} \equiv a \cdot x_n^{-1} + b \pmod{2^e}, \qquad x_{n+1} \in \mathbf{Z}_{2^e},\ n \geq 0,$$

is studied, where $e \geq 3$ and $a, b, x_0 \in \mathbf{Z}_{2^e} = \{0, 1, \ldots, 2^e - 1\}$ with $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, and $x_0 \equiv 1 \pmod 2$. Then $x_n \equiv 1 \pmod 2$, $n \geq 0$, and hence the inverse element x_n^{-1} of x_n in $\mathbf{Z}_{2^e}$ is well defined, and the generator (2) is purely periodic. In this note a simple necessary and sufficient condition is derived for this generator to have the maximal period length 2^{e-1}.

2. Maximal Period Length. The following technical lemma is used in the proof of the Theorem.

LEMMA. *Consider the matrix*

$$A = \begin{pmatrix} 0 & 1 \\ 4\alpha + 1 & 4\beta + 2 \end{pmatrix}$$

Received October 27, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C10; Secondary 11K45.
Key words and phrases. Pseudorandom number generator, nonlinear congruential sequence, power of two modulus, period length.

for some fixed nonnegative integers α *and* β. *Then*

$$A^{2^{f-1}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^f(\alpha+\beta)+1 \\ 2^f(\alpha+\beta+1)+1 \end{pmatrix} \pmod{2^{f+1}} \tag{3}$$

for every $f \geq 3$.

Proof. A short calculation shows that

$$A^4 = \begin{pmatrix} 16\gamma_3 + 8\alpha + 5 & 16\delta_3 + 8\beta + 12 \\ 16\varepsilon_3 + 8\beta + 12 & 16\eta_3 + 8\alpha + 13 \end{pmatrix}$$

for some nonnegative integers $\gamma_3, \delta_3, \varepsilon_3$ and η_3. It then follows by induction that

$$A^{2^{f-1}} = \begin{pmatrix} \gamma_f \cdot 2^{f+1} + \alpha \cdot 2^f + 2^{f-1} + 1 & \delta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} \\ \varepsilon_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} & \eta_f \cdot 2^{f+1} + \alpha \cdot 2^f + 3 \cdot 2^{f-1} + 1 \end{pmatrix}$$

for some nonnegative integers $\gamma_f, \delta_f, \varepsilon_f, \eta_f$ and every $f \geq 3$, which yields (3). □

THEOREM. *A nonlinear generator* (2) *has maximal period length* 2^{e-1} *if and only if*

$$a \equiv 1 \pmod 4 \quad \text{and} \quad b \equiv 2 \pmod 4. \tag{4}$$

Proof. In what follows, $x_0 = 1$ is assumed without loss of generality. First, it is assumed that the generator (2) has maximal period length 2^{e-1} for some $e \geq 3$. Hence, it has period length 2 for $e = 2$ and period length 4 for $e = 3$. Therefore, $x_2 \equiv 1 \pmod 4$ and hence $x_2 \equiv 5 \pmod 8$. Since $x^{-1} \equiv x \pmod 8$ for $x \in \{1, 3, 5, 7\}$, it follows that

$$x_2 \equiv a(a+b) + b \equiv (a+1)b + 1 \pmod 8. \tag{5}$$

Therefore, $(a+1)b \equiv 4 \pmod 8$ which yields (4).

Now we assume that conditions (4) are satisfied. It will be shown by induction that the generator (2) has period length 2^{f-1} modulo 2^f for every integer f with $3 \leq f \leq e$. For $f = 3$, this follows at once from (4) and (5). If it is valid for some f with $3 \leq f \leq e-1$, then

$$x_n \not\equiv 1 \pmod{2^{f+1}}, \qquad n \in \mathbf{Z}_{2^f} \backslash \{0, 2^{f-1}\}.$$

Since the generator (2) is purely periodic, it suffices to show that

$$x_{2^{f-1}} \equiv 2^f + 1 \pmod{2^{f+1}}. \tag{6}$$

Put $y_0 = y_1 = 1$ and define

$$y_n \equiv b y_{n-1} + a y_{n-2} \pmod{2^e}, \qquad y_n \in \mathbf{Z}_{2^e},\ n \geq 2. \tag{7}$$

Since $a+b \equiv 1 \pmod 2$, it follows that $y_n \equiv 1 \pmod 2$, $n \geq 0$. Therefore (7) implies that

$$y_{n+1} \cdot y_n^{-1} \equiv a(y_n \cdot y_{n-1}^{-1})^{-1} + b \pmod{2^e}, \qquad n \geq 1.$$

Hence $x_0 = y_0 = y_1 = 1$, and (2) shows that

$$x_n \equiv y_{n+1} \cdot y_n^{-1} \pmod{2^e}, \qquad n \geq 0. \tag{8}$$

Because of (4) there exist nonnegative integers α and β such that $a = 4\alpha + 1$ and $b = 4\beta + 2$. Therefore (7) yields

$$\begin{pmatrix} y_n \\ y_{n+1} \end{pmatrix} \equiv A^n \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{2^e}, \qquad n \geq 0,$$

where the matrix A is defined as in the lemma. Hence, the lemma implies that

$$y_{2^{f-1}} \equiv 2^f(\alpha + \beta) + 1 \pmod{2^{f+1}}$$

and

$$y_{2^{f-1}+1} \equiv 2^f(\alpha + \beta + 1) + 1 \pmod{2^{f+1}}.$$

Since $y_{2^{f-1}}^{-1} \equiv y_{2^{f-1}} \pmod{2^{f+1}}$, it follows by (8) that (6) is valid. □

Acknowledgment. The authors are indebted to Professor Knuth for his suggestion to study the nonlinear generators in this paper. They also wish to thank Holger Grothe and Rainer Weilbächer for valuable hints and the Deutsche Forschungsgemeinschaft for financial support.

Fachbereich Mathematik
Technische Hochschule Darmstadt
Schlossgartenstrasse 7
D-6100 Darmstadt, West Germany

Department of Mathematics
Middle East Technical University
Ankara, Turkey

1. W. A. BEYER, R. B. ROOF & D. WILLIAMSON, "The lattice structure of multiplicative pseudo-random vectors," *Math. Comp.*, v. 25, 1971, pp. 345–363.

2. J. EICHENAUER & J. LEHN, "A non-linear congruential pseudorandom number generator," *Statist. Hefte*, v. 27, 1986, pp. 315–326.

3. J. EICHENAUER & J. LEHN, "On the structure of quadratic congruential sequences," *Manuscripta Math.*, v. 58, 1987, pp. 129–140.

4. J. EICHENAUER, H. GROTHE & J. LEHN, "Marsaglia's lattice test and non-linear congruential pseudorandom number generators," *Metrika*, 1988. (To appear.)

5. J. EICHENAUER, H. GROTHE, J. LEHN & A. TOPUZOĞLU, "A multiple recursive nonlinear congruential pseudorandom number generator," *Manuscripta Math.*, v. 59, 1987, pp. 331–346.

6. D. E. KNUTH, *The Art of Computer Programming*, vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

7. D. E. KNUTH, personal communication, 1986.

→ G. MARSAGLIA, "Random numbers fall mainly in the planes," *Proc. Nat. Acad. Sci. U.S.A.*, v. 61, 1968, pp. 25–28.