Journal of Computational and Applied Mathematics 31 (1990) 81–85
North-Holland

On the lattice structure of a nonlinear generator with modulus 2^α

J. EICHENAUER–HERRMANN, H. GROTHE
Fachbereich Mathematik, Technische Hochschule, Schloßgartenstraße 7, D-6100 Darmstadt, FRG

H. NIEDERREITER
Institut für Informationsverarbeitung, Österreichische Akademie der Wissenschaften, Sonnenfelsgasse 19, A-1010 Wien, Austria

A. TOPUZOĞLU
Department of Mathematics, Middle East Technical University, Ankara, Turkey

Received 17 March 1989

Abstract: Nonlinear congruential pseudorandom number generators based on inversions have been introduced and analysed recently. These generators do not show the simple lattice structure of the widely used linear congruential generators which are too regular for certain simulation purposes. In the present paper a nonlinear congruential generator based on inversions with respect to a power of two modulus is considered. It is shown that the set of points formed by consecutive pseudorandom numbers has a more complicated lattice structure: it forms a superposition of shifted lattices. The corresponding lattice bases are explicitly determined and analysed.

Keywords: Pseudorandom numbers, nonlinear congruential method, inversion modulo 2^α, lattice structure, superposition of lattices.

Let $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ and $\mathbb{Z}_{2^\alpha}^* = \{1, 3, \ldots, 2^\alpha - 1\}$ for $m, \alpha \in \mathbb{N}$. Suppose $a, b \in \mathbb{Z}_{2^\alpha}$, $a \equiv 1 \pmod 4$, and $b \equiv 2 \pmod 4$. Define a nonlinear generator by

$$x_{n+1} \equiv a \cdot x_n^{-1} + b \pmod{2^\alpha}, \quad n \geqslant 0, \tag{1}$$

where x^{-1} is the unique element in $\mathbb{Z}_{2^\alpha}^*$ satisfying $x \cdot x^{-1} \equiv 1 \pmod{2^\alpha}$ for $x \in \mathbb{Z}_{2^\alpha}^*$ and where $x_0 \in \mathbb{Z}_{2^\alpha}^*$. The conditions on a, b, x_0 guarantee that (1) has maximal period length $2^{\alpha-1}$ (see [2]).

Let $\mathbb{Z}^*$ be the set of odd integers. Define $f_n : \mathbb{Z}^* \to \mathbb{Z}_{2^\alpha}^*$, $n \geqslant 0$, by

$$f_0(x) \equiv x \pmod{2^\alpha}, \qquad f_1(x) \equiv a \cdot x^{-1} + b \pmod{2^\alpha},$$
$$f_n(x) \equiv f_1(f_{n-1}(x)), \quad n \geqslant 2.$$

For $d \in \mathbb{N}$, $d \geqslant 2$, define $\eta \in \mathbb{Z}_\alpha$ such that $2^\eta = \gcd(d, 2^{\alpha-1})$. Let

$$V_{d,x_0} = \left\{ \left(f_{j \cdot d}(x_0), \ldots, f_{j \cdot d + d - 1}(x_0) \right) \mid j \in \mathbb{Z}_{2^{\alpha-1-\eta}} \right\}$$
$$= \left\{ \left(f_{j \cdot 2^\eta}(x_0), \ldots, f_{j \cdot 2^\eta + d - 1}(x_0) \right) \mid j \in \mathbb{Z}_{2^{\alpha-1-\eta}} \right\}$$

be the set of nonoverlapping d-dimensional vectors which are generated by (1).

Lemma 1. *$f_{2^\beta}(x) \equiv x \pmod{2^{\beta+1}}$ for $\beta \in \mathbb{Z}_\alpha$ and $x \in \mathbb{Z}_{2^\alpha}^*$.*

Proof. The case $\beta = 0$ is obvious, since $f_1(x) \equiv x \equiv 1 \pmod 2$ for every $x \in \mathbb{Z}_{2^\alpha}^*$. If $\beta \geqslant 1$, let $\tilde{a}$, $\tilde{b} \in \mathbb{Z}_{2^{\beta+1}}$ be such that $\tilde{a} \equiv a \pmod{2^{\beta+1}}$ and $\tilde{b} \equiv b \pmod{2^{\beta+1}}$. Then $\tilde{a} \equiv 1 \pmod 4$ and $\tilde{b} \equiv 2 \pmod 4$, which implies that the nonlinear generator

$$x_{n+1} \equiv \tilde{a} \cdot x_n^{-1} + \tilde{b} \pmod{2^{\beta+1}}, \quad n \geqslant 0,$$

has maximal period length 2^β, i.e.,

$$f_{2^\beta}(x) \equiv x \pmod{2^{\beta+1}}$$

for every $x \in \mathbb{Z}_{2^{\beta+1}}^*$. □

Let $x_0' \in \mathbb{Z}_{2^{\eta+1}}^*$, $x_0' \equiv x_0 \pmod{2^{\eta+1}}$. Put

$$\mathbb{Z}_{2^\alpha}(2^{\eta+1}, x_0') = \{x \in \mathbb{Z}_{2^\alpha}^* \mid x = 2^{\eta+1} \cdot y + x_0',\ y \in \mathbb{Z}_{2^{\alpha-\eta-1}}\}.$$

By Lemma 1, the set V_{d,x_0} can be written in the form

$$V_{d,x_0} = \{(x, f_1(x), \ldots, f_{d-1}(x)) \mid x \in \mathbb{Z}_{2^\alpha}(2^{\eta+1}, x_0')\},$$

and hence it suffices to consider starting values $x_0 \in \mathbb{Z}_{2^{\eta+1}}^*$. Let

$$G_{d,x_0} = \{\vec{g} \in \mathbb{Z}^d \mid \vec{g} = \vec{v} + 2^\alpha \cdot \vec{u},\ \vec{v} \in V_{d,x_0},\ \vec{u} \in \mathbb{Z}^d\}$$

be the periodic continuation of V_{d,x_0} with period 2^α. Put $\omega = \max([\frac{1}{2}(\alpha+1)], \eta+1)$ and

$$V_d(z) = \{(x, f_1(x), \ldots, f_{d-1}(x)) \mid x \in \mathbb{Z}_{2^\alpha}(2^\omega, z)\}$$

for $z \in \mathbb{Z}_{2^\omega}^*$. Let

$$G_d(z) = \{\vec{g} \in \mathbb{Z}^d \mid \vec{g} = \vec{v} + 2^\alpha \cdot \vec{u},\ \vec{v} \in V_d(z),\ \vec{u} \in \mathbb{Z}^d\}$$

be the periodic continuation of $V_d(z)$ with period 2^α. Obviously the sets $G_d(z)$, $z \in \mathbb{Z}_{2^\omega}^*$, are mutually disjoint and

$$G_{d,x_0} = \bigcup_{z \in \mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)} G_d(z)$$

for any starting value $x_0 \in \mathbb{Z}_{2^{\eta+1}}^*$. It is proved below that each set $G_d(z)$ for $z \in \mathbb{Z}_{2^\omega}^*$ is a grid, i.e., a shifted lattice, and hence the set G_{d,x_0} is a superposition of $2^{\omega-\eta-1}$ subgrids for every starting value $x_0 \in \mathbb{Z}_{2^{\eta+1}}^*$. Define functions $\alpha_n : \mathbb{Z}_{2^\alpha}^* \to \mathbb{Z}_{2^\alpha}^*$, $n \in \mathbb{N}$, by

$$\alpha_n(z) \equiv (-a)^n \cdot (z \cdot f_1(z) \cdot \ldots \cdot f_{n-1}(z))^{-2} \pmod{2^\alpha}.$$

Lemma 2. *Let $z \in \mathbb{Z}_{2^\omega}^*$. Then*

$$f_n(x) \equiv \alpha_n(z) \cdot (x - z) + f_n(z) \pmod{2^\alpha} \tag{2}$$

for all $n \in \mathbb{N}$ and $x \in \mathbb{Z}_{2^\alpha}(2^\omega, z)$.

Proof. Suppose $z \in \mathbb{Z}_{2^\alpha}^*$ and $x = 2^\omega \cdot y + z$ for some $y \in \mathbb{Z}$. Let z^{-1} be the inverse of z in $\mathbb{Z}_{2^\alpha}^*$. Put $x^{-1} = -2^\omega \cdot y \cdot z^{-2} + z^{-1}$. Then $x \cdot x^{-1} \equiv 1 \pmod{2^\alpha}$ since $2 \cdot \omega \geqslant \alpha$. Hence

$$f_1(2^\omega \cdot y + z) \equiv \alpha_1(z) \cdot 2^\omega \cdot y + f_1(z) \pmod{2^\alpha}. \tag{3}$$

If $z \in \mathbb{Z}_{2^\omega}^*$ and $x = 2^\omega \cdot y + z \in \mathbb{Z}_{2^\alpha}(2^\omega, z)$, then (2) is the same as (3) for $n = 1$. If (2) holds for some $n \geqslant 1$, then applying (3) one gets

$$\begin{aligned} f_{n+1}(x) &\equiv f_1(f_n(x)) \equiv f_1(\alpha_n(z) \cdot 2^\omega \cdot y + f_n(z)) \\ &\equiv \alpha_1(f_n(z)) \cdot \alpha_n(z) \cdot 2^\omega \cdot y + f_1(f_n(z)) \\ &\equiv \alpha_{n+1}(z) \cdot (x - z) + f_{n+1}(z) \pmod{2^\alpha}. \end{aligned}$$ □

Theorem 3. *The set $G_d(z)$ is a grid with shift vector*

$$\vec{g}_0(z) = (z, f_1(z), \ldots, f_{d-1}(z))$$

and the basis

$$\begin{aligned} \vec{g}_1(z) &= 2^\omega \cdot (1, \alpha_1(z), \ldots, \alpha_{d-1}(z)), \\ \vec{g}_2(z) &= (0, 2^\alpha, 0, \ldots, 0), \\ &\vdots \\ \vec{g}_d(z) &= (0, 0, \ldots, 0, 2^\alpha). \end{aligned}$$

The theorem follows by an argument similar to that of the proof of the theorem in [1], using Lemma 2.

Summarising one can state the following result.

Result. For any starting value $x_0 \in \mathbb{Z}_{2^{\eta+1}}^*$ the set G_{d,x_0} is a superposition of $2^{\omega-\eta-1}$ grids $G_d(z)$, $z \in \mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$.

Remark 4. If $\omega = \eta + 1$, i.e., $\eta + 1 \geqslant [\frac{1}{2}(\alpha + 1)]$, then the set G_{d,x_0} is a pure grid, since $\mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$ consists of one element.

It is analysed below whether in the case $\omega = [\frac{1}{2}(\alpha + 1)] > \eta + 1$ some of the sets $G_d(z)$ are spanned by the same basis when z varies over $\mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$.

Lemma 5. *Let $d \geqslant 3$, $\alpha \geqslant 3$, $\omega = [\frac{1}{2}(\alpha + 1)]$, $z, \tilde{z} \in \mathbb{Z}_{2^\omega}^*$. Then*

(i) $z^2 \equiv \tilde{z}^2 \pmod{2^{\alpha-\omega}}$,

and

(ii) $z \equiv \tilde{z} \pmod{2^{\alpha-\omega-2}}$,

if and only if

$$(f_n(z))^2 \equiv (f_n(\tilde{z}))^2 \pmod{2^{\alpha-\omega}} \quad \text{and} \quad f_n(z) \equiv f_n(\tilde{z}) \pmod{2^{\alpha-\omega-2}}, \qquad n \geqslant 0.$$

Proof. The lemma is proved by induction. That (i) and (ii) hold if and only if

$$(f_0(z))^2 \equiv (f_0(\tilde{z}))^2 \pmod{2^{\alpha-\omega}} \quad \text{and} \quad f_0(z) \equiv f_0(\tilde{z}) \pmod{2^{\alpha-\omega-2}}$$

is obvious. Now assume that

$$(f_n(z))^2 \equiv (f_n(\tilde{z}))^2 \pmod{2^{\alpha-\omega}} \quad \text{and} \quad f_n(z) \equiv f_n(\tilde{z}) \pmod{2^{\alpha-\omega-2}}$$

for some $n \geqslant 0$. Then

$$\begin{aligned}(f_{n+1}(z))^2 &\equiv \left(a^2 + 2 \cdot a \cdot b \cdot f_n(z) + b^2 \cdot (f_n(z))^2\right) \cdot (f_n(z))^{-2} \\ &\equiv \left(a^2 + 2 \cdot a \cdot b \cdot f_n(\tilde{z}) + b^2 \cdot (f_n(\tilde{z}))^2\right) \cdot (f_n(\tilde{z}))^{-2} \\ &\equiv (f_{n+1}(\tilde{z}))^2 \pmod{2^{\alpha-\omega}}, \quad \text{since } b \equiv 2 \pmod 4\end{aligned}$$

and

$$\begin{aligned}f_{n+1}(z) &\equiv a \cdot (f_n(z))^{-1} + b \equiv a \cdot (f_n(\tilde{z}))^{-1} + b \\ &\equiv f_{n+1}(\tilde{z}) \pmod{2^{\alpha-\omega-2}}, \quad \text{since } f_n(z) \equiv 1 \pmod 2. \qquad \square\end{aligned}$$

Lemma 6. *The congruence* $z^2 \equiv \epsilon^2 \pmod{2^\alpha}$ *has exactly four different solutions in* $\mathbb{Z}_{2^\alpha}^*$, $\alpha \geqslant 3$, *for* $\epsilon \in \mathbb{Z}_{2^\alpha}^*$, *namely*:

$$\begin{aligned}z_1 &\equiv \epsilon \pmod{2^\alpha}, & z_2 &\equiv 2^{\alpha-1} + \epsilon \pmod{2^\alpha}, \\ z_3 &\equiv -\epsilon \pmod{2^\alpha}, & z_4 &\equiv 2^{\alpha-1} - \epsilon \pmod{2^\alpha}.\end{aligned}$$

Proof. Consider the congruence $x^2 \equiv 1 \pmod{2^\alpha}$. Then $(x+1) \cdot (x-1) \equiv 0 \pmod{2^\alpha}$ and hence

$$x + 1 \equiv 0 \pmod{2^\beta} \quad \text{and} \quad x - 1 \equiv 0 \pmod{2^{\alpha-\beta}}$$

for some suitable integer β with $1 \leqslant \beta \leqslant \alpha - 1$. Therefore

$$x = 2^\beta \cdot \gamma - 1 \quad \text{and} \quad x = 2^{\alpha-\beta} \cdot \delta + 1$$

for some integers γ and δ. But these equations are satisfied only for $\beta = 1$ or $\beta = \alpha - 1$. If $\beta = 1$, then either $\delta = 0$ or $\delta = 1$ and hence $x_1 = 1$ and $x_2 = 2^{\alpha-1} + 1$. If $\beta = \alpha - 1$, then $\gamma = 0$ or $\gamma = 1$ and hence $x_3 = -1$ and $x_4 = 2^{\alpha-1} - 1$. The result follows by putting $x \equiv z \cdot \epsilon^{-1} \pmod{2^\alpha}$. $\square$

Theorem 7. *Let* $\omega = [\frac{1}{2}(\alpha+1)] > \eta + 1$.

(I) *If* $3 \leqslant \alpha \leqslant 7$, *then all the sets* $G_d(z)$ *are spanned by the same basis for* $z \in \mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$.

(II) *If* $\alpha \geqslant 8$, *then exactly two lattice bases are equal if either* $\alpha \equiv 0 \pmod 2$ *or* $\alpha \equiv 1 \pmod 2$ *and* $\omega = \eta + 2$, *and exactly four lattice bases are equal if* $\alpha \equiv 1 \pmod 2$ *and* $\omega > \eta + 2$.

Proof. (I) If $3 \leqslant \alpha \leqslant 7$, then for $\omega = [\frac{1}{2}(\alpha+1)]$ it follows that $\alpha - \omega \leqslant 3$ and hence $\vec{g}_1(z) \equiv \vec{g}_1(\tilde{z}) \pmod{2^\alpha}$ for all $z, \tilde{z} \in \mathbb{Z}_{2^\omega}^*$, since the congruences (i) and (ii) of Lemma 5 are always satisfied as $z^2 \equiv 1 \pmod 8$ for $z \equiv 1 \pmod 2$.

(II) First consider the case $d \geqslant 3$. Suppose $z, \tilde{z} \in \mathbb{Z}_{2^\omega}^*$. Put $\alpha_0(z) \equiv 1 \pmod{2^\alpha}$. Then $\alpha_{n+1}(z) \equiv -a \cdot (f_n(z))^{-2} \cdot \alpha_n(z) \pmod{2^\alpha}$. Hence it follows from Lemma 5 that

(i) $\quad z^2 \equiv \tilde{z}^2 \pmod{2^{\alpha-\omega}}$,

and

(ii) $\quad z \equiv \tilde{z} \pmod{2^{\alpha-\omega-2}}$,

if and only if $\alpha_i(z) \equiv \alpha_i(\tilde{z}) \pmod{2^{\alpha-\omega}}$ for $1 \leqslant i \leqslant d-1$. Therefore $G_d(z)$ and $G_d(\tilde{z})$ are spanned by the same basis if and only if (i) and (ii) above are satisfied. By Lemma 6 the congruence $z^2 \equiv \epsilon^2 \pmod{2^{\alpha-\omega}}$ has solutions

$$\begin{aligned}z_1 &\equiv \epsilon \pmod{2^{\alpha-\omega}}, & z_2 &\equiv 2^{\alpha-\omega-1} + \epsilon \pmod{2^{\alpha-\omega}}, \\ z_3 &\equiv -\epsilon \pmod{2^{\alpha-\omega}}, & z_4 &\equiv 2^{\alpha-\omega-1} - \epsilon \pmod{2^{\alpha-\omega}} \quad \text{for } \epsilon \in \mathbb{Z}_{2^{\alpha-\omega}}^*.\end{aligned}$$

Obviously $z_1 \equiv z_2 \pmod{2^{\alpha-\omega-2}}$, $z_3 \equiv z_4 \pmod{2^{\alpha-\omega-2}}$ and $z_1 \not\equiv z_3 \pmod{2^{\alpha-\omega-2}}$ since $\alpha - \omega - 2 \geqslant 2$.

If $\alpha \equiv 0 \pmod 2$, i.e., $\omega = \alpha - \omega = \frac{1}{2}\alpha$ and $\tilde{z} \in \mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$, then $z_1 \equiv \tilde{z} \pmod{2^\omega}$ and $z_2 \equiv 2^{\alpha-\omega-1} + \tilde{z} \pmod{2^\omega}$ are the only solutions of the congruences (i) and (ii), since the other solutions $z_3 \equiv -\tilde{z} \pmod{2^\omega}$ and $z_4 \equiv 2^{\alpha-\omega-1} - \tilde{z} \pmod{2^\omega}$ of (i) do not satisfy (ii). It is obvious that $z_1 \equiv z_2 \equiv \tilde{z} \equiv x_0 \pmod{2^{\eta+1}}$, since $\eta + 1 < \omega$.

If $\alpha \equiv 1 \pmod 2$, i.e., $\omega = \alpha - \omega + 1 = \frac{1}{2}(\alpha + 1)$ and $\tilde{z} \in \mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$, it follows, as in the case of $\alpha \equiv 0 \pmod 2$, that $z_1 \equiv \tilde{z} \pmod{2^\omega}$, $z_2 \equiv 2^{\alpha-\omega-1} + \tilde{z} \pmod{2^\omega}$, $z_3 \equiv 2^{\alpha-\omega} + z_1 \pmod{2^\omega}$, and $z_4 \equiv 2^{\alpha-\omega} + z_2 \pmod{2^\omega}$ are the solutions of the congruences (i) and (ii). If $\omega > \eta + 2$, then all four solutions belong to $\mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$, and if $\omega = \eta + 2$, then only z_1 and z_3 belong to $\mathbb{Z}_{2^\omega}(2^{\eta+1}, x_0)$.

In the case $d = 2$, (i) is equivalent to $\vec{g}_1(z) \equiv \vec{g}_1(\tilde{z}) \pmod{2^\alpha}$. It can be shown similarly to the case of $d \geqslant 3$ that (i) has exactly four solutions for $\alpha \equiv 0 \pmod 2$ and exactly eight solutions for $\alpha \equiv 1 \pmod 2$. Since $\eta = 1$ and $-x_0 \not\equiv x_0 \pmod 4$ only half of these solutions satisfy the congruence $z \equiv x_0 \pmod 4$. □

References

[1] J. Eichenauer and J. Lehn, On the structure of quadratic congruential sequences, *Manuscripta Math.* **58** (1987) 129–140.

[2] J. Eichenauer, J. Lehn and A. Topuzoğlu, A nonlinear congruential pseudorandom number generator with power of two modulus, *Math. Comp.* **51** (1988) 757–759.