manuscripta math. 58, 129 - 140 (1987)

manuscripta
mathematica
© Springer-Verlag 1987

ON THE STRUCTURE OF QUADRATIC CONGRUENTIAL SEQUENCES

Jürgen Eichenauer and Jürgen Lehn

Sequences of integers defined by a quadratic congruential formula are divided into non-overlapping subsequences of length d. The structure of the set of the resulting points in the d-dimensional Euclidean space $\mathbb{R}^d$ is studied. The analysis is restricted to the case of sequences with maximal period length since such sequences are of special interest in connection with pseudo random number generation.

1. Introduction

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

$$(1) \qquad x_{n+1} \equiv b \cdot x_n + c (\mathrm{mod}\ m), \quad 0 \le x_{n+1} < m, \quad n \ge 0,$$

where m is a (large) positive integer and x_o, b, and c are non-negative integers less than m. This type of generators goes back to Lehmer [8] and Rotenberg [12].

If the generator (1) has maximal period length m it is well known (see e.g. [3], [4], [5], [7], [10] and [11]) that the vectors

$$(x_o, x_1, \dots, x_{d-1}),\ (x_1, x_2, \dots, x_d),\ \dots$$

of d consecutive pseudo random numbers form a shifted lattice, so-called a grid, in the Euclidean space $\mathbb{R}^d$.

Moreover Afflerbach [1] showed that the vectors of non-overlapping d-sequences

$$(x_o,x_1,\dots,x_{d-1}),\ (x_d,\dots,x_{2d-1}),\ \dots$$

form a grid in $\mathbb{R}^d$.

These results made it possible to develop numerical methods for determining generators with a "good" lattice structure (see e.g. [2], [3], [4] and [5]) by adjusting the parameters m, b and c.

Marsaglia [9] however regards this lattice structure as a defect caused by the linearity of (1). In [6] a simulation problem is described which supports Marsaglia's judgement. This suggests the study of non-linear congruential sequences. Results on the period length for certain non-linear congruential generators are given in [6] and are also known for quadratic congruential generators of the form

$$(2)\qquad x_{n+1} \equiv a\cdot x_n^2 + b\cdot x_n + c(\mathrm{mod}\ m),\quad 0 \le x_{n+1} < m,\quad n \ge 0,$$

where m is a positive integer, x_o, b, and c are non-negative integers less than m, and a is a positive integer less than or equal to m (see Knuth [7], p. 25).

In this paper the structure of the set of all vectors

$$(3)\qquad (x_o,x_1,\dots,x_{d-1}),\ (x_d,x_{d+1},\dots,x_{2d-1}),\ \dots$$

of non-overlapping d-sequences generated by (2) will be discussed in the case of the quadratic congruential generator (2) with maximal period length m.

The proof of the main result of this paper follows the ideas in Afflerbach [1].

2. Notation and definitions

Let $m = p_1^{m_1}\cdot\ldots\cdot p_k^{m_k}$ denote the factorization of the modulus m into prime numbers with $p_1 < p_2 < \ldots < p_k$. Then the quadratic congruential generator (2) has maximal period length m if and only if the following conditions are fulfilled (see [7], p. 34, and p. 526):

(4) (i) c is relatively prime to m,

(ii) $a \equiv 0 \pmod{p_i}$ and $b \equiv 1 \pmod{p_i}$ for every prime factor $p_i \geq 3$, $1 \leq i \leq k$,

(iii) $a \equiv b-1 \pmod{2}$ if $p_1 = 2$ and $m_1 = 1$,
$a \equiv b-1 \pmod{4}$ and $a \equiv 0 \pmod{2}$ if $p_1 = 2$ and $m_1 \geq 2$ and

(iv) $a \equiv 0 \pmod{9}$ or $a \cdot c \equiv 6 \pmod{9}$ if 9 divides m.

The second condition $b \equiv 1 \pmod{9}$ in the or-part of (iv) given in [7] is not necessary.

Here the quadratic congruential generators are assumed to have maximal period length. Without loss of generality $a \equiv b-1 \equiv 0 \pmod{2}$ if $p_1 = 2$ and $m_1 = 1$ since $x^2 \equiv x \pmod{2}$. Then there exist positive integers $a_o, a_1, \ldots, a_k$ with $a_i \leq m_i$ and $a_o \not\equiv 0 \pmod{p_i}$ for $1 \leq i \leq k$ and

$$a = a_o \cdot p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}.$$

Let

$$\mu = p_1^{\mu_1} \cdot \ldots \cdot p_k^{\mu_k}$$

be the divisor of m with

$$\mu_i = [(m_i - a_i + 1)/2], \quad 1 \leq i \leq k,$$

where $[y]$ denotes the greatest integer less than or equal to y. For every positive integer n let

$$Z(n) = \{0, 1, \ldots, n-1\}$$

denote the set of all non-negative integers less than n. For every positive integer n, divisor t of n, and $z \in Z(t)$ let

$$Z_n(t,z) = \{y \cdot t + z \in Z(n) \mid y \in Z(n/t)\}$$

be a subset of $Z(n)$. For every non-negative integer n define a function f_n on $Z(m)$ by

$$f_n(x) = f_1(f_{n-1}(x)), \quad n \geq 2,$$

$$f_1(x) \equiv a \cdot x^2 + b \cdot x + c \pmod{m}, \quad 0 \leq f_1(x) < m, \quad \text{and}$$

$$f_o(x) = x.$$

Then $f_n(x)$ is the nth successor of x when the quadratic congruential generator (2) is applied. For every positive integer n define a function α_n on $Z(m)$ by

$$\alpha_n(x) = \alpha_1(f_{n-1}(x)) \cdot \alpha_{n-1}(x), \quad n \geq 2, \quad \text{and}$$

$$\alpha_1(x) = 2ax + b.$$

For some fixed integer $d \geq 2$ let

$$e = \gcd(d,m)$$

be the greatest common divisor of d and m and let

$$\nu = \operatorname{lcm}(e,\mu)$$

be the least common multiple of e and μ defined above. Since e divides m there exist non-negative integers $e_1,\dots,e_k$ with $e_i \leq m_i$, $1 \leq i \leq k$, and

$$e = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}.$$

Thus

$$\nu = p_1^{\nu_1} \cdot \ldots \cdot p_k^{\nu_k}$$

with $\nu_i = \max(e_i,\mu_i)$, $1 \leq i \leq k$. Define

$$\lambda_i = \max(m_i - \nu_i - a_i,\ e_i), \quad 1 \leq i \leq k,$$

and

$$\lambda = \begin{cases} p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot \ldots \cdot p_k^{\lambda_k} & \text{for } p_1 \geq 3 \\ p_1^{\max(\lambda_1-1,e_1)} \cdot p_2^{\lambda_2} \cdot \ldots \cdot p_k^{\lambda_k} & \text{for } p_1 = 2. \end{cases}$$

$2\mu_i \geq m_i - a_i$ and $\mu_i \leq \nu_i$ show that $m_i - \nu_i - a_i \leq 2\mu_i - \nu_i \leq \nu_i$, $1 \leq i \leq k$. This and $e_i \leq \nu_i$ give $\lambda_i \leq \nu_i$, $1 \leq i \leq k$, i.e. λ divides ν. It is easy to show that $\lambda = \nu$ if and only if

(5) $\mu_1 \leq e_1$ for $p_1 = 2$ and

$\mu_i \leq e_i$ or

$\mu_i > e_i$ and $m_i - a_i$ is even for $p_i \geq 3$, $1 \leq i \leq k$,

are satisfied. For every $x_o \in Z(m)$ let

$$V_{d,x_o} = \{(f_{jd}(x_o), \ldots, f_{jd+d-1}(x_o)) \mid j \in Z(m/e)\}$$

denote the set of all vectors (3) generated by the quadratic congruential generator (2) with starting value x_o. Since e divides m by Lemma 1 below

$$V_{d,x_o} = \{(x, f_1(x), \ldots, f_{d-1}(x)) \mid x \in Z_m(e, x_o')\}$$

where $x_o' \in Z(e)$ is an integer with $x_o' \equiv x_o \pmod{e}$. Therefore $x_o \in Z(e)$ is assumed without loss of generality. For every $x_o \in Z(e)$ let

$$G_{d,x_o} = \{g = v + m \cdot u \in \mathbb{Z}^d \mid v \in V_{d,x_o},\ u \in \mathbb{Z}^d\}$$

be the periodic continuation with period m of V_{d,x_o} where $\mathbb{Z}^d$ denotes the set of all d-tupels of integers. For every $z \in Z(\nu)$ let

$$V_d(z) = \{(x, f_1(x), \ldots, f_{d-1}(x)) \mid x \in Z_m(\nu, z)\}$$

be a subset of V_{d,x_o} for some $x_o \in Z(e)$ and let

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

be the periodic continuation with period m of $V_d(z)$. It is obvious that the sets $V_d(z)$, $z \in Z(\nu)$, and $G_d(z)$, $z \in Z(\nu)$, are pairwise disjoint, and that for every $x_o \in Z(e)$

$$V_{d,x_o} = \bigcup_{z \in Z_\nu(e,x_o)} V_d(z) \quad \text{and}$$

$$G_{d,x_o} = \bigcup_{z \in Z_\nu(e,x_o)} G_d(z)$$

since e divides ν. Given $g_o,\dots,g_d \in \mathbb{R}^d$ where $g_1,\dots,g_d$ are linearly independent, the set

$$G = \{g = g_o + u_1 g_1 + \dots + u_d g_d \in \mathbb{R}^d \mid u_1,\dots,u_d \in \mathbb{Z}\}$$

is called a grid or shifted lattice with basis $g_1,\dots,g_d$, and g_o is called the shift-vector.

In the sequel it will be shown that $G_d(z)$ forms a grid for every $z \in Z(\nu)$. Therefore G_{d,x_o} is a superimposition of ν/e grids for every $x_o \in Z(e)$.

3. Some technical lemmas

LEMMA 1. *Let the parameters* a, b, *and* c *in the definition of the function* f_1 *satisfy conditions* (4). *Let* t *be a positive integer dividing* m. *Then*

$$f_t(x) \equiv x \pmod t$$

for every $x \in Z(t)$.

PROOF. Since t divides m there are non-negative integers $t_i \le m_i$, $1 \le i \le k$, with

$$t = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}.$$

Now it is easy to check that the conditions (4) are also fulfilled with the modulus t instead of m. Therefore the quadratic congruential generator (2) with modulus t instead of m has maximal period length t. Thus it follows from the definition of the function f_t that

$$f_t(x) \equiv x \pmod{t}$$

for every $x \in Z(t)$. □

LEMMA 2. Let the parameters a, b, *and* c *in the definition of the function* f_1 *satisfy conditions* (4).
Then for every $z \in Z(\mu)$ *and* $x \in Z_m(\mu,z)$

$$f_n(x) \equiv \alpha_n(z) \cdot (x-z) + f_n(z) \pmod{m}$$

for all positive integers n.

PROOF. The lemma is proved for fixed $z \in Z(\mu)$ and $x = y \cdot \mu + z \in Z_m(\mu,z)$ by induction on n. The definition of f_1 and the factorizations of a and μ show

$$\begin{aligned} f_1(x) &\equiv a \cdot (y \cdot \mu + z)^2 + b \cdot (y \cdot \mu + z) + c \\ &\equiv a_o \cdot y^2 \cdot p_1^{a_1+2\mu_1} \cdot \ldots \cdot p_k^{a_k+2\mu_k} \\ &\quad + (2 \cdot a \cdot z + b) \cdot y \cdot \mu + a \cdot z^2 + b \cdot z + c \\ &\equiv \alpha_1(z) \cdot (x-z) + f_1(z) \pmod{m} \end{aligned}$$

since $2\mu_i + a_i \geq m_i$, $1 \leq i \leq k$, by the definition of $\mu_1, \ldots, \mu_k$. Thus the assertion is valid for $n = 1$.

Now assume that the assertion is valid for $1 \leq j \leq n-1$ and some fixed $n \geq 2$. Then it follows from the definition of f_n and α_n, and the factorization of a and μ that

$$\begin{aligned} f_n(x) &\equiv f_1(f_{n-1}(x)) \\ &\equiv a \cdot (\alpha_{n-1}(z) \cdot y \cdot \mu + f_{n-1}(z))^2 + b \cdot (\alpha_{n-1}(z) \cdot y \cdot \mu + f_{n-1}(z)) + c \\ &\equiv a_o \cdot \alpha_{n-1}^2(z) \cdot y^2 \cdot p_1^{a_1+2\mu_1} \cdot \ldots \cdot p_k^{a_k+2\mu_k} \\ &\quad + (2 \cdot a \cdot f_{n-1}(z) + b) \cdot \alpha_{n-1}(z) \cdot y \cdot \mu \\ &\quad + a \cdot f_{n-1}^2(z) + b \cdot f_{n-1}(z) + c \end{aligned}$$

$$\equiv \alpha_1(f_{n-1}(z)) \cdot \alpha_{n-1}(z) \cdot y \cdot \mu + f_1(f_{n-1}(z))$$

$$\equiv \alpha_n(z) \cdot (x-z) + f_n(z) \pmod{m}. \qquad \square$$

LEMMA 3. *For every* $s \in Z(\lambda)$ *and* $z_1, z_2 \in Z_\nu(\lambda,s)$

$$\nu \cdot (1,\alpha_1(z_1),\ldots,\alpha_{d-1}(z_1)) \equiv \nu \cdot (1,\alpha_1(z_2),\ldots,\alpha_{d-1}(z_2)) \pmod{m}.$$

PROOF. Let some $s \in Z(\lambda)$ and $z_1, z_2 \in Z_\nu(\lambda,s)$ be fixed. By the definition of α_1 and λ and the factorization of a

$$\alpha_1(z_1) \equiv \alpha_1(z_2) \pmod{m/\nu}.$$

The assumption $z_1, z_2 \in Z_\nu(\lambda,s)$ yields $f_n(z_1) \equiv f_n(z_2) \pmod{\lambda}$ for every positive integer n. Thus

$$\alpha_n(z_1) \equiv \alpha_n(z_2) \pmod{m/\nu}$$

for every positive integer n by the definition of α_n. This proves the lemma. $\square$

4. Main results

The main result of this paper is formulated in the following theorem. By Lemma 2 it can be shown that the set $G_d(z)$ is a grid for every $z \in Z(\nu)$.

THEOREM. *Let the parameters* a, b, *and* c *in the definition of the function* f_1 *satisfy conditions* (4). *Then for every* $z \in Z(\nu)$ *the set* $G_d(z)$ *is a grid in the Euclidean space* $\mathbb{R}^d$ *with shift-vector*

$$g_o(z) = (z,f_1(z),\ldots,f_{d-1}(z))$$

and basis

$$g_1(z) = \nu \cdot (1,\alpha_1(z),\ldots,\alpha_{d-1}(z)),$$
$$g_2(z) = (0,m,0,\ldots,0),$$
$$\vdots$$
$$g_d(z) = (0,0,\ldots,0,m).$$

PROOF. Let $z \in Z(\nu)$ be fixed. Let g denote some element of the set $G_d(z)$. By the definition of $G_d(z)$ and $V_d(z)$

$$g = (x,f_1(x),\ldots,f_{d-1}(x)) + m \cdot u$$

for some $x \in Z_m(\nu,z)$ and $u \in \mathbb{Z}^d$. Now μ divides ν and ν divides m since $\nu = \mathrm{lcm}(e,\mu)$, $e = \gcd(d,m)$, and μ divides m. Therefore Lemma 2 shows that

$$g = (1,\alpha_1(z),\ldots,\alpha_{d-1}(z)) \cdot (x-z) + (z,f_1(z),\ldots,f_{d-1}(z)) + m \cdot u.$$

Define the integers

$$\tilde{u}_1 = (x - z + m \cdot u_1)/\nu,$$
$$\tilde{u}_2 = u_2 - u_1 \cdot \alpha_1(z),$$
$$\vdots$$
$$\tilde{u}_d = u_d - u_1 \cdot \alpha_{d-1}(z).$$

Then g can be written in the form

$$\begin{aligned} g &= (z,f_1(z),\ldots,f_{d-1}(z)) \\ &\quad + (\nu\tilde{u}_1,\nu\tilde{u}_1\alpha_1(z) + m\tilde{u}_2,\ldots,\nu\tilde{u}_1\alpha_{d-1}(z) + m\tilde{u}_d) \\ &= g_o(z) + \tilde{u}_1\nu(1,\alpha_1(z),\ldots,\alpha_{d-1}(z)) + (0,\tilde{u}_2m,\ldots,\tilde{u}_dm) \\ &= g_o(z) + \tilde{u}_1g_1(z) + \tilde{u}_2g_2(z) + \ldots + \tilde{u}_dg_d(z). \end{aligned}$$

Now assume

$$g = g_o(z) + \tilde{u}_1g_1(z) + \ldots + \tilde{u}_dg_d(z)$$

for some integers $\tilde{u}_1,\ldots,\tilde{u}_d$. Then define

$$
\begin{aligned}
u_1 &= [\tilde{u}_1 \nu/m],\\
u_2 &= \tilde{u}_2 + u_1\alpha_1(z),\\
&\ \vdots\\
u_d &= \tilde{u}_d + u_1\alpha_{d-1}(z),
\end{aligned}
$$

and $y = \tilde{u}_1 - u_1 m/\nu \in Z(m/\nu)$. Thus $x = y\nu + z \in Z_m(\nu,z)$ and

$$
\begin{aligned}
g &= (z,f_1(z),\ldots,f_{d-1}(z))\\
&\quad + (\tilde{u}_1\nu,\ \tilde{u}_1\nu\alpha_1(z) + \tilde{u}_2 m,\ldots,\tilde{u}_1\nu\alpha_{d-1}(z) + \tilde{u}_d m)\\
&= (z,f_1(z),\ldots,f_{d-1}(z))\\
&\quad + (y\nu + u_1 m,\ (y\nu + u_1 m)\alpha_1(z) + \tilde{u}_2 m,\ldots,(y\nu + u_1 m)\alpha_{d-1}(z) + \tilde{u}_d m)\\
&= (1,\alpha_1(z),\ldots,\alpha_{d-1}(z))\cdot(x-z) + (z,f_1(z),\ldots,f_{d-1}(z)) + m\cdot u.
\end{aligned}
$$

Therefore Lemma 2 shows that

$$g = (x,f_1(x),\ldots,f_{d-1}(x)) + m\cdot u \in G_d(z).$$

Since $|\det(g_1(z),\ldots,g_d(z))| = \nu m^{d-1}$ the vectors $g_1(z),\ldots,g_d(z)$ are linearly independent and form a basis of the grid $G_d(z)$. □

The Theorem and Lemma 3 yield the following

RESULT. *For every* $x_o \in Z(e)$ *the periodic continuation* G_{d,x_o} *with period* m *of the set* V_{d,x_o} *of all vectors* (3) *of non-overlapping d-sequences generated by the quadratic congruential generator* (2) *with starting value* x_o *is a superimposition of* ν/e *grids* $G_d(z)$, $z \in Z_\nu(e,x_o)$, *as are described in the Theorem.*

For every $s \in Z_\lambda(e,x_o)$ *there are* ν/λ *grids* $G_d(z)$, $z \in Z_\nu(\lambda,s)$, *having the same basis but different shift-vectors.*

5. Remarks

For $a \equiv 0 \pmod{m}$, i.e. in the linear case, the Result coincides with that in [1].

To get more information about the distribution of non-overlapping vectors (3) generated by the quadratic congruential generator (2) the basis $g_1(z),\ldots,g_d(z)$ of the grids $G_d(z)$, $z \in Z(\nu)$, have to be reduced to bases with vectors of minimal length (see e.g. [3], [4], and [5]). In [2] a fast algorithm for the calculation of reduced lattice bases is presented.

If the number ν/e of grids $G_d(z)$, $z \in Z_\nu(e,x_o)$, forming the superimposition G_{d,x_o} is small the parameters a, b, and c of the quadratic congruential generator (2) should be chosen in such a way that the reduced lattice bases of all grids consist of vectors of nearly the same length. If ν/e is large the reduced lattice bases of most if not all grids should have this property.

The following example illustrates the Result. In the case of the quadratic congruential generator

$$x_{n+1} \equiv 2461 \cdot x_n^2 + 7200 \cdot x_n + 1 \pmod{23^4}, \quad 0 \le x_{n+1} < 23^4, \quad n \ge 0,$$

and dimensions d with $d \not\equiv 0 \pmod{23}$ the set G_{d,x_o} is a superimposition of 23^2 grids $G_d(z)$, $z \in Z(23^2)$, as described in the Theorem. For every $s \in Z(23)$ there are 23 grids $G_d(z)$, $z \in Z_{23^2}(23,s)$, having the same basis but different shift-vectors.

Acknowledgement

The authors would like to thank Dr. Topuzoğlu for valuable suggestions and a referee for his careful reading the manuscript. They also wish to thank the Deutsche Forschungsgemeinschaft for financial support.

References

[1] Afflerbach, L.: The sub-lattice structure of linear congruential random number generators, manuscripta math. 55, 455-465 (1986)

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

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

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

[5] Dieter, U. and Ahrens, J.H.: Uniform random numbers, Institut f. Math. Stat., Technische Hochschule Graz (1974)

[6] Eichenauer, J. and Lehn, J.: A non-linear congruential pseudo random number generator. Fachbereich Mathematik, Technische Hochschule Darmstadt, Preprint Nr. 988 (1986); Statistical Papers (to appear)

[7] Knuth, D.E.: The art of computer programming, vol. 2, 2nd ed., Addison-Wesley 1981

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

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

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

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

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

Jürgen Eichenauer
Jürgen Lehn
Fachbereich Mathematik der
Technischen Hochschule Darmstadt
Schlossgartenstr. 7
D - 6100 Darmstadt

(Received October 23, 1986;
in revised form January 21, 1987)