HAL open science

# Spectral Analysis of the MIXMAX Random Number Generators

Pierre L'Ecuyer, Paul Wambergue, Erwan Bourceret

**To cite this version:**

Pierre L'Ecuyer, Paul Wambergue, Erwan Bourceret. Spectral Analysis of the MIXMAX Random Number Generators. 2017. hal-01634350v1

**HAL Id: hal-01634350**

**https://inria.hal.science/hal-01634350v1**

Preprint submitted on 14 Nov 2017 (v1), last revised 10 Dec 2018 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Spectral Analysis of the MIXMAX Random Number Generators

Pierre L'Ecuyer[1], Paul Wambergue, and Erwan Bourceret

Département d'Informatique et de Recherche Opérationnelle, Université de Montréal Pavillon Aisenstadt, C.P. 6128, Succ. Centre-Ville, Montréal (Québec), H3C 3J7, CANADA, {lecuyer@iro.umontreal.ca, paul.wambergue@gmail.com, ebourceret@hotmail.fr}

We study the lattice structure of random number generators of the MIXMAX family, a class of matrix linear congruential generators that produce a vector of random numbers at each step. These generators were initially proposed and justified as close approximations to certain ergodic dynamical systems having the Kolmogorov K-mixing property, which implies a chaotic (fast-mixing) behavior. But for a K-mixing system, the matrix must have irrational entries, whereas for the MIXMAX it has only integer entries. As a result, the MIXMAX has a lattice structure just like linear congruential and multiple recursive generators. Its matrix entries were also selected in a special way to allow a fast implementation and this has an impact on the lattice structure. We study this lattice structure for vectors of successive and non-successive output values in various dimensions. We show in particular that for coordinates at specific lags not too far apart, in three dimensions, all the nonzero points lie in only two hyperplanes. This is reminiscent of the behavior of lagged-Fibonacci and AWC/SWB generators. And even if we skip the output coordinates involved in this bad structure, other highly structured projections often remain, depending on the choice of parameters.

*Key words:* Random number generators, matrix linear congruential generators, lattice structure, spectral test, simulation

**This version:** September 22, 2017

---

## 1. Introduction

A *matrix linear congruential generator* (matrix LCG) of *order* $k$ with *modulus* $m$ evolves according to a linear recurrence of the form

$$\mathbf{x}_i \;=\; \mathbf{A}\mathbf{x}_{i-1} \bmod m \tag{1}$$

in which $\mathbf{x}_i = (x_{i,0}, \ldots, x_{i,k-1})^{\mathsf{t}}$ is a $k$-dimensional column vector (the $^{\mathsf{t}}$ means *transposed*) with coordinates in $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, and $\mathbf{A}$ is a $k \times k$ matrix with elements in $\mathbb{Z}_m$.

The vector $\mathbf{x}_i \in \mathbb{Z}_m^k$ is the *state* of the generator at step $i$. The total number of possible states is $m^k$, and since we must avoid the absorbing state $\mathbf{0}$, the period of the recurrence cannot exceed $m^k - 1$. This period is attained if and only if $m$ is a prime number and the characteristic polynomial of $\mathbf{A}$ is a primitive polynomial modulo $m$ (Niederreiter, 1986). The output at step $i$ is the following $k$-dimensional vector of random numbers $u_{i,j} \in [0, 1)$:

$$\mathbf{u}_i = (u_{i,0}, \ldots, u_{i,k-1}) = \mathbf{x}_i/m \in [0, 1)^k. \tag{2}$$

Matrix LCGs have been discussed and studied in Tahmi (1982); Niederreiter (1986); Grothe (1988); L'Ecuyer (1990, 1994), for example.

The MIXMAX generators are matrix LCGs with special choices of $\mathbf{A}$. They were introduced by Akopov et al. (1991) and Savvidy and Ter-Arutyuntan-Savvidy (1991), and further developed in Savvidy (2015) and Savvidy and Savvidy (2016). The original version proposed by Akopov et al. (1991) had

$$\mathbf{A} = \mathbf{A}(m, k, d) = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 3+d & 2 & 1 & \cdots & 1 & 1 \\ 1 & 4 & 3 & 2 & \cdots & 1 & 1 \\ \vdots & & & & \ddots & & \\ 1 & k & k-1 & k-2 & \cdots & 3 & 2 \end{pmatrix}, \tag{3}$$

in which $d \geq 0$ is an integer parameter that can be chosen in addition to the dimension $k$ and the modulus $m$. We shall call it the MIXMAX-$(m, k, d)$.

This construction of $\mathbf{A}$ was selected to satisfy the following two conditions: (1) the determinant of $\mathbf{A}$ is 1 and (2) the eigenvalues $\lambda_1, \ldots, \lambda_k$ of $\mathbf{A}$ are away from the unit circle. The first condition implies that the linear transformation defined by $\mathbf{A}$ (modulo $m$) over the hypercube $[0, m)^k$ in the real space transforms any region $R \subseteq [0, m)^k$ into another region of the same volume. The second condition ensures that trajectories that start from states very close to each other and evolve according to this transformation in the real space diverge exponentially fast. This speed of divergence is related to the Kolmogorov entropy defined as

$$h = \sum_{j=1}^{k} \mathbb{I}[|\lambda_j| > 1] \cdot \log |\lambda_j|,$$

where $\mathbb{I}$ is the indicator function. Savvidy (2015) provides lower bounds on $h$ that depend only on $k$, for the MIXMAX-$(m, k, d)$, and shows that $h$ is reasonably large. In particular, $h$ is much larger than for the AWC and SWB generators of Marsaglia and Zaman (1991).

Savvidy (2015) also shows that the maximal period for these generators is $(m^k - 1)/(m - 1)$, which is $m - 1$ times shorter than the maximal possible period for matrix LCGs. This limitation stems from the requirement that $\det(\mathbf{A}) = 1$. He provides a table of parameters $(k, d)$ for $m = 2^{61} - 1$ where $k$ ranges from 10 to 3150, $d$ ranges from $-11$ to 15, and the period is $(m^k - 1)/(m - 1)$ divided by a small integer (which is 1 in some cases). He finally provides an efficient implementation that uses only $2k$ additions and one multiplication by $d$ to compute the next vector $\mathbf{x}_i$ at each step.

To increase the flexibility and eventually permit a larger entropy and potentially better behavior, Savvidy and Savvidy (2016) defined a MIXMAX variant with an additional integer parameter $c$, with

$$\mathbf{A} = \mathbf{A}(m, k, d, c) = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & c+2+d & 2 & 1 & \cdots & 1 & 1 \\ 1 & 2c+2 & c+2 & 2 & \cdots & 1 & 1 \\ 1 & 3c+2 & 2c+2 & c+2 & \cdots & 1 & 1 \\ & & & \cdots & & & \\ 1 & (k-2)c+2 & (k-3)c+2 & (k-4)c+2 & \cdots & c+2 & 2 \end{pmatrix}, \quad (4)$$

which we call MIXMAX-$(m, k, d, c)$, and another variant with five parameters $(m, k, d, c, b)$, with

$$\mathbf{A} = \mathbf{A}(m, k, d, c, b) = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 3c+d+b & 2 & 1 & \cdots & 1 & 1 \\ 1 & 4c+b & 3c+b & 2 & \cdots & 1 & 1 \\ 1 & 5c+b & 4c+b & 3c+b & \cdots & 1 & 1 \\ & & & \cdots & & & \\ 1 & kc+b & (k-1)c+b & (k-2)c+b & \cdots & 3c+b & 2 \end{pmatrix}, \quad (5)$$

which we denote by MIXMAX-$(m, k, d, c, b)$. These generators also satisfy the conditions (1) and (2) above and have the same maximal possible period as the MIXMAX-$(m, k, d)$. Note that in those papers, the parameters $m, k, d, c$ are named $p, N, s, m$ instead. A user's guide with specific parameters and pointers to downloadable code is available in Savvidy (2017). This code is also part of the ROOT library available at the CERN, in Geneva.

Examining the eigenvalues of $\mathbf{A}$ and the entropy $h$ is one type of spectral analysis for matrix LCGs. A different type of spectral analysis is the *spectral test* that examines the lattice structure of vectors of successive or non-successive output values produced by LCGs (Coveyou and MacPherson, 1967; Knuth, 1998; L'Ecuyer and Couture, 1997). The purpose

of this paper is to show how this spectral test applies to MIXMAX generators and see what kind of lattice structure we can find.

The remainder is organized as follows. In Section 2, we recall the lattice structure of matrix LCGs and how the spectral test works for these generators. In Section 3, we prove various properties of the lattice structure of the MIXMAX generators. We show that certain coordinates of the successive output points are linked by very simple linear relations, which implies that these points belong to a small number of parallel hyperplanes in the unit hypercube. We illustrate this with specific MIXMAX generators proposed in Savvidy (2017).

For general background on uniform random number generators (RNGs), we refer the reader to the recent reviews by L'Ecuyer (2012) and L'Ecuyer et al. (2017), and the detailed historical account of L'Ecuyer (2017).

## 2. Lattice Structure of matrix LCGs

Suppose a matrix LCG produces $s$ uniform random numbers $u_0, \ldots, u_{s-1}$ as follows. Starting from some initial state $\mathbf{x}_0$, we generate $\mathbf{u}_0, \ldots, \mathbf{u}_{\nu-1}$ as in (2) where $\nu$ satisfies $s = k\nu + r$ and $r < k$, and we put $u_{ki+j} = u_{i,j}$ for all $i = 0, \ldots, \nu$ and $j = 0, \ldots, k-1$ for which $0 \le ki - j < s$. Let $\Psi_s$ be the set of all vectors $(u_0, \ldots, u_{s-1})$ obtained in this way, from all the $m^k$ possible initial states $\mathbf{x}_0$ of the matrix LCG, including the zero vector. In case the generator does not have full period $m^k - 1$, the set $\Psi_s$ considered here contains all vectors produced over all cycles of the generator. An important requirement of good RNGs is that this set $\Psi_s$ covers the unit hypercube $[0, 1)^s$ very evenly, at least when $s$ is not too large (L'Ecuyer, 1994, 2006). This requirement captures uniformity and independence of the successive random numbers. Note that for $s = k$, $\Psi_s$ contains all the $m^k$ points of $\mathbb{Z}_m^k/m = \{0, 1/m, \ldots, (m-1)/m\}^k$ exactly once. For $s < k$, $\Psi_s$ is a multiset that contains all points $\mathbb{Z}_m^s/m$ exactly $m^{k-s}$ times each.

We also consider the following generalized form of this notion, as in Couture and L'Ecuyer (1994); L'Ecuyer and Couture (1997), and L'Ecuyer and Simard (2014). For any finite set of integers $I = \{i_1, \ldots, i_s\}$ where $0 \le i_1 < \cdots < i_s$, consider the multiset $\Psi_s(I)$ of all $s$-dimensional output vectors $(u_{i_1}, \ldots, u_{i_s})$ obtained by the method described earlier, from all possible initial states $\mathbf{x}_0$:

$$\Psi_s(I) = \{(u_{i_1}, \ldots, u_{i_s}) \in [0, 1)^s \mid \mathbf{x}_0 \in \mathbb{Z}_m^k\}.$$

If $\mathbf{x}_0$ is selected randomly and uniformly from $\mathbb{Z}_m^k$, then $(u_{i_1}, \ldots, u_{i_s})$ has the uniform distribution over the multiset $\Psi_s(I)$. This can be a good approximation of the uniform distribution over $[0,1)^s$ only if $\Psi_s(I)$ covers $[0,1)^s$ very evenly. This multiset $\Psi_s(I)$ is actually the projection of the set $\Psi_{s'}$ over the selected coordinate indices $i_1, \ldots, i_s$, with $s' = i_s + 1$. The set $\Psi_s$ is just a special case of this with $I = \{0, ..., s-1\}$.

It is known that any projection $\Psi_s(I)$ of some $\Psi_{s'}$ over a subset of $s$ coordinates, is the (finite) intersection of a lattice $L_s(I)$ in the real space $\mathbb{R}^s$ with the unit hypercube $[0,1)^s$ (Afflerbach and Grothe, 1988; L'Ecuyer and Couture, 1997). One consequence of this is that there are families of equidistant parallel hyperplanes in $\mathbb{R}^s$ such that each family contains all the points of $\Psi_s(I)$. We want to make sure that none of these families has just a few widely-spaced hyperplanes, because this would imply that the points would not cover the space very well. The *spectral test* introduced by Coveyou and MacPherson (1967) for LCGs and further discussed in Knuth (1998) and L'Ecuyer and Couture (1997), for example, computes the distance $d_s(I)$ between successive hyperplanes for the family for which this distance is largest. Let $n = \min(m^k, m^s)$, which is the largest number of distinct points that we can have in $\Psi_s(I)$. A standardized figure of merit whose value is always between 0 and 1 regardless of $n$ and $s$ can be defined as $S_s(I) = d_s^*(n)/d_s(I)$, where $d_s^*(n)$ is a tight lower bound on the distance between hyperplanes that can be achieved by a general $s$-dimensional lattice having $n$ points per unit of volume (Conway and Sloane, 1999; L'Ecuyer, 1999). Very small values of $S_s(I)$ are bad and should be avoided.

It is also known that $d_s(I) = 1/\ell_s(I)$ where $\ell_s(I)$ is the (Euclidean) length of the shortest nonzero vector in the dual lattice

$$L_s^*(I) = \{\mathbf{w} \in \mathbb{R}^s : \mathbf{w}^\mathsf{t}\mathbf{v} \bmod 1 = 0 \text{ for all } \mathbf{v} \in L_s(I)\}.$$

To compute a shortest vector and its length, one first constructs a basis of the dual lattice. Then the shortest vector and its length are a solution and the optimal value of a quadratic integer optimization problem that can be solved by a branch-and-bound procedure (Fincke and Pohst, 1985; L'Ecuyer and Couture, 1997).

If we compute the shortest nonzero vector in the dual lattice with the $L^1$ norm defined by $\|\mathbf{w}\|_1 = \|(w_1, \ldots, w_s)\|_1 = |w_1| + \cdots + |w_s|$ instead of the Euclidean norm, the length of the shortest vector minus one gives the minimal number of hyperplanes that cover all the lattice points in $[0,1)^s$ (Marsaglia, 1968; Knuth, 1998).

The lattice bases can be constructed as follows. Suppose $s = k\nu + r$ and for any $k \times k$ matrix $\mathbf{M}$, let $[\mathbf{M}]_r$ denote the $r \times k$ matrix formed by the first $r$ rows of $\mathbf{M}$. Let $\mathbf{I}$ be the identity matrix. Consider the $s \times s$ matrices

$$\mathbf{V} = \begin{pmatrix} \mathbf{I}/m & \mathbf{A}^{\mathsf{t}}/m & \cdots & (\mathbf{A}^{\nu-1})^{\mathsf{t}}/m & ([\mathbf{A}^{\nu}]_r)^{\mathsf{t}}/m \\ \mathbf{0} & \mathbf{I} & & & \mathbf{0} \\ & & \ddots & & \\ & & & \mathbf{I} & \\ \mathbf{0} & & & & \mathbf{I} \end{pmatrix} \tag{6}$$

and

$$\mathbf{W} = \begin{pmatrix} m \cdot \mathbf{I} & \mathbf{0} & & \mathbf{0} \\ -\mathbf{A} & \mathbf{I} & & \\ \vdots & & \ddots & \\ -\mathbf{A}^{\nu-1} & & \mathbf{I} & \\ -[\mathbf{A}^{\nu}]_r & \mathbf{0} & & \mathbf{I} \end{pmatrix} \tag{7}$$

in which the identity $\mathbf{I}$ at the bottom right of each matrix is $r \times r$ and the other $\mathbf{I}$'s are $k \times k$. Then the rows of $\mathbf{V}$ form a basis of the lattice $L_s$ (Afflerbach and Grothe, 1988) and, since $\mathbf{V}\mathbf{W}^{\mathsf{t}} = \mathbf{I}$, the rows of $\mathbf{W}$ form the corresponding dual basis, which is a basis of the dual lattice $L_s^*$. Any integer linear combination of the rows of $\mathbf{W}$ belongs to the dual lattice.

For the case of lacunary indices, a set of generating vectors for $L_s(I)$ can be obtained by projecting the basis vectors of $L_{s'}$ over the $s$ retained coordinates in $I$. That is, we build $\mathbf{V}$ with $s'$ columns and then we keep only the columns of $\mathbf{V}$ whose indices are in $I$, and discard the other ones. The $s'$ rows of the resulting matrix give a set of $s'$ vectors that can be turned into a set of $s$ independent vectors that form a basis of $L_s(I)$, using the approach described in L'Ecuyer and Couture (1997). The corresponding dual basis can then be obtained by inverting this basis matrix modulo 1. (Note that projecting the vectors of the original dual basis on the retained lacunary coordinates *does not* provide vectors that belong to the dual basis of $L_s(I)$ in general.)

# 3. Lattice Structure of MIXMAX

When a MIXMAX generator has maximal period, it has $m-1$ cycles of length $(m^k-1)/(m-1)$, and the initial state determines which cycle we are in. In this paper, we study the lattice $L_s$ or $L_s(I)$ generated by all the points produced over all the cycles of the MIXMAX generator. Since the generator can have many disjoint cycles, it could perhaps happen that the lattice generated by a single cycle is a strict sublattice of the full lattice generated by all the points

produced over all the cycles. Analyzing the lattice generated over a single cycle is beyond the scope of the present paper. It could be done using the ideas and methodology of Couture and L'Ecuyer (1996).

By writing the matrix $-\mathbf{A} = -\mathbf{A}(m,k,d)$ explicitly in rows $k+1$ to $2k$ of the definition of $\mathbf{W}$, we find that for the MIXMAX-$(m,k,d)$,

$$\mathbf{W} = \begin{pmatrix} & m\cdot\mathbf{I} & & & & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ -1 & -1 & -1 & \cdots & -1 & & & & \\ -1 & -2 & -1 & \cdots & -1 & & & & \\ -1 & -3-d & -2 & \cdots & -1 & \mathbf{I} & \mathbf{0} & \cdots & \mathbf{0} \\ -1 & -4 & -3 & \cdots & -1 & & & & \\ & & & \cdots & & & & & \\ -1 & -k & -(k-1) & \cdots & -2 & & & & \\ & -\mathbf{A}^2 & & & & \mathbf{0} & \mathbf{I} & & \\ & \vdots & & & & \vdots & & \ddots & \\ & -\mathbf{A}^{\nu-1} & & & & & & & \\ & -[\mathbf{A}^{\nu}]_r & & & & \mathbf{0} & & & \mathbf{I} \end{pmatrix}.$$

For the MIXMAX-$(m,k,d,c)$ and MIXMAX-$(m,k,d,c,b)$, it suffices to replace the explicit submatrix $-\mathbf{A} = -\mathbf{A}(m,k,d)$ in $\mathbf{W}$ by either $-\mathbf{A}(m,k,d,c)$ or $-\mathbf{A}(m,k,d,c,b)$. The rows of $\mathbf{W}$, which we denote by $\mathbf{w}_1,\ldots,\mathbf{w}_s$, form a basis of the dual lattice, so any integer linear combination of these vectors belongs to the dual lattice $L_s^*$.

In particular, if $k \geq 2$, we have

$$\mathbf{w}_{k+1} = (-1,-1,-1,\ldots,-1,1,0,\ldots,0)$$
$$\mathbf{w}_{k+2} = (-1,-2,-1,\ldots,-1,0,1,\ldots,0)$$
$$\uparrow \text{ coordinate } k+1$$

and therefore

$$\mathbf{w} = \mathbf{w}_{k+1} - \mathbf{w}_{k+2} = (0,1,0,\ldots,0,1,-1,0,\ldots,0)$$
$$\uparrow \text{ coordinate } k+1$$

is in the dual lattice $L_s^*$ for any $s \geq k+2$. (Here, the index $i$ of output values and the coordinates of $\mathbf{u}_i$ start at 0 as usual, but we start the coordinates of vectors $\mathbf{v}$ and $\mathbf{w}$ at 1, which is also standard.) This vector $\mathbf{w}$ has Euclidean length $\sqrt{3}$ and $L^1$ norm equal to 3. Its presence in the dual lattice implies that if we take all $k$ output values at each step, the successive output values satisfy $(u_1 + u_k - u_{k+1}) \mod 1 = 0$. And since $0 \leq u_i < 1$ for all $i$, one must have $u_1 + u_k - u_{k+1} = q$ for $q \in \{0, 1\}$. This means that if we take $I = \{1, k, k+1\}$, all the points of $\Psi_3(I)$ are in only two planes, determined by this equation. Also, the dual lattice to $L_3(I)$ contains the vector $(1, 1, -1)$, whose Euclidean length is $\sqrt{3}$. This argument holds in exactly the same way for the MIXMAX-$(m, k, d, c)$ and MIXMAX-$(m, k, d, c, b)$ as well, because they have the same first two rows of $\mathbf{A}$. We have just proved the following.

**Proposition 1** *For the three MIXMAX variants, with $k \geq 2$, for $I = \{1, k, k+1\}$, all the points of $\Psi_3(I)$ are in two equidistant parallel planes, which are at distance $1/\sqrt{3}$ apart, in the three dimensional unit hypercube. This also holds more generally for $\Psi_s(I)$ in the $s$-dimensional unit hypercube if $\{1, k, k+1\} \subseteq I$.*

The following proposition applies to the MIXMAX-$(m, k, d)$ only. If $k \geq 5$, by taking

$$\mathbf{w} = \mathbf{w}_{2k} - \mathbf{w}_{2k-1} - \mathbf{w}_{k+1} = (1, 0, \ldots, 0, -1, 0, \ldots, 0, -1, 1, 0, \ldots, 0)$$
$$\uparrow \text{ coord. } k+1$$

in which we have $-1$ at coordinates $k+1$ and $2k-1$, we find with a similar reasoning:

**Proposition 2** *For the MIXMAX-$(k, d)$ with $k \geq 5$, if $\{0, k, 2k-2, 2k-1\} \subseteq I$, then all the points of $\Psi_s(I)$ are in the three equidistant parallel planes with equations $u_0 - u_k - u_{2k-2} + u_{2k-1} = q$ for $q \in \{-1, 0, 1\}$, which are at distance $1/2$ apart.*

Note that in contrast to the previous one, this relationship does not involve the second coordinate of the state vectors of size $k$. One can find other relationships like this and we will give a few more in what follows.

# 4. Skipping coordinates

The simplest way to eliminate the bad structure exhibited in the previous propositions is to skip some coordinates of the $k$-dimensional vector $\mathbf{u}_i$ when producing the output. Instead of taking all $k$ coordinates at each step, one can retain only a subset $J \subset \{0, \ldots, k-1\}$ of

the $k$ coordinates, to produce a block of $|J|$ random numbers at each step. For example, if we skip the second coordinate of each vector, i.e., if we take $J = \{0, 2, 3, \ldots, k-1\}$, the relationship $u_1 + u_k - u_{k+1} = 0$ or 1 is not harmful anymore, because $u_1$ and $u_{k+1}$ are no longer used. But other relationships can be found that do not involve these removed coordinates (Proposition 2 gives one), and some of these relationships may correspond to short vectors in the dual of the corresponding projected lattice $L_s(I)$, where $I$ contains only coordinates that are retained. To find such a relationship, we need to find a vector $\mathbf{w} \in L_s^*$ whose coordinates that correspond to the output values that are skipped are zero. (In the notation used in this paper, the indices of the $u_i$'s when we skip coordinates remain the same as when we take all $k$ values at each step; we find this less confusing than making them depend on $I$ of $J$.)

If the set $J$ of coordinates that we keep includes the first two coordinates, then the relationship $u_1 + u_k - u_{k+1} = 0$ or 1 still involves coordinates that are all retained and the bad lattice structure remains. To remove this structure, one must skip at least one of the first two coordinates. For the MIXMAX-$(m, k, d)$, if we skip only the second coordinate of each $\mathbf{u}_i$, the problem remains, because the relationship in Proposition 2 does not involve $u_1, u_{k+1}, u_{2k+1}, \ldots$, so we still have the bad hyperplane structure pointed out in this proposition.

The next proposition shows that even if we skip the first two (and even the first three) coordinates of each $\mathbf{u}_i$, for the MIXMAX-$(m, k, d)$ we still get bad relationships among the other coordinates, and therefore a bad structure.

**Proposition 3** *For the MIXMAX-$(m, k, d)$, if $k \geq 6$, $0 \leq j \leq k-6$, and $\{5+j, k+3+j, k+4+j, k+5+j\} \subseteq I$, then $\Psi_s(I)$ is contained in at most 4 equidistant parallel hyperplanes at distance $1/\sqrt{7}$ apart. If $k \geq 7$, $0 \leq j \leq k-7$, and the stronger condition $\{5+j, 6+j, k+3+j, k+4+j, k+5+j, k+6+j\} \subseteq I$ holds, then $\Psi_s(I)$ is also contained in 5 equidistant parallel hyperplanes at distance $1/\sqrt{6}$ apart. Note that these 5 hyperplanes are not the same as the 4 hyperplanes in the first part.*

**Proof.** For the first part, take

$$\mathbf{w} = \mathbf{w}_{k+4+j} - 2\mathbf{w}_{k+5+j} + \mathbf{w}_{k+6+j} = (0, \ldots, 0, \underset{\uparrow\ \text{coord. } 6+j}{-1}, 0, \ldots, 0, 1, -2, 1, 0, \ldots).$$

in which the $-1$ is at position $6+j$ and the $-2$ is at position $k+5+j$. This shows that we have the relationship $-u_{5+j} + u_{k+3+j} - 2u_{k+4+j} + u_{k+5+j} = q$ for $q \in \{-2, -1, 0, 1\}$. These

are the equations of four hyperplanes that contain all the points of $\Psi_s(I)$ when $I$ contains the coordinates involved in this linear relationship. In this case, the lattice $L_s(I)$ contains a dual vector with $L^1$-norm of 5 and Euclidean length $\sqrt{7}$.

For the second part, take

$$\mathbf{w} = \mathbf{w}_{k+4+j} - \mathbf{w}_{k+5+j} - \mathbf{w}_{k+6+j} + \mathbf{w}_{k+7+j} = (0, \ldots, 0, -1, -1, 0, \ldots, 0, 1, -1, -1, 1, 0, \ldots).$$
$$\uparrow \text{ coord. } 6+j$$

in which the first $-1$ is at position $6+j$ and the first 1 is at position $k+4+j$. This dual basis vector indicates the relationship $-u_{5+j} - u_{6+j} + u_{k+3+j} - u_{k+4+j} - u_{k+5+j} + u_{k+6+j} = q$ for $q \in \{-3, -2, -1, 0, 1\}$, which involves only retained coordinates if $I$ satisfies the condition in the second part of the proposition. Then the lattice $L_s(I)$ contains a dual vector with $L^1$-norm of 6 and Euclidean length $\sqrt{6}$, and the conclusion follows. Since the condition of the second part implies that of the first part, the result of the first part also holds here. The two sets of hyperplanes are different. □

By taking for $\mathbf{w}$ the same combination of dual vectors as in the first part of the previous Proposition, we obtain the following two results for the MIXMAX with four and five parameters. In all the propositions that follow, $\ell$ will denote the length of a short vector in the dual lattice, but not necessarily the shortest length.

**Proposition 4** *For the MIXMAX-$(m, k, d, c)$ generator with $c \geq 1$, if $k \geq 6$, $0 \leq j \leq k-6$, and $\{4+j, 5+j, k+3+j, k+4+j, k+5+j\} \subseteq I$, then there is a set of $c+3$ equidistant parallel hyperplanes that contain all the points of $\Psi_s(I)$. These hyperplanes are at distance $1/\ell$ apart, where $\ell^2 = (c-1)^2 + 7$.*

**Proof.** The dual basis contains the vector

$$\mathbf{w} = \mathbf{w}_{k+4+j} - 2\mathbf{w}_{k+5+j} + \mathbf{w}_{k+6+j} = (0, \ldots, 0, 1-c, -1, 0, \ldots, 0, 1, -2, 1, 0, \ldots),$$
$$\uparrow \text{ coord. } 5+j$$

in which the $1-c$ is at position $5+j$ and the $-2$ is at position $k+5+j$. Thus we have the relationship $(1-c)u_{4+j} - u_{5+j} + u_{k+3+j} - 2u_{k+4+j} + u_{k+5+j} = q$ where $q \in \{-c-1, -c, \ldots, 0, 1\}$. Also, the square Euclidean length of $\mathbf{w}$ is $(c-1)^2 + 7$. The result follows. □

**Proposition 5** *For the MIXMAX-$(m, k, d, c, b)$ generator with $c \geq 1$ and $b \geq 0$, if $k \geq 6$, $0 \leq j \leq k-6$, and $\{3+j, 4+j, 5+j, k+3+j, k+4+j, k+5+j\} \subseteq I$, then there is a set of $5c+2b-1$ equidistant parallel hyperplanes that contain all the points of $\Psi_s(I)$. These hyperplanes are at distance $1/\ell$ apart, where $\ell^2 = (2c+b-2)^2 + (3c+b-3)^2 + 7$.*

**Proof.** The dual lattice contains

$$\mathbf{w} = \mathbf{w}_{k+4+j} - 2\mathbf{w}_{k+5+j} + \mathbf{w}_{k+6+j} = (0, \ldots, 0, 2c+b-2, -3c-b+3, -1, 0, \ldots, 0, 1, -2, 1, 0, \ldots)$$
$$\uparrow \text{ coord. } 4+j$$

in which the $-2$ is at position $k+5+j$. Thus, $((2c+b-2)u_{3+j} - (3c+b-3)u_{4+j} - u_{5+j} + u_{k+3+j} - 2u_{k+4+j} + u_{k+5+j}) \bmod 1 = 0$. If $I$ contains the coordinates involved in this linear relationship, the lattice $L_s(I)$ contains a dual vector with $L^1$-norm of $5c+2b$ and square Euclidean length $(2c+b-2)^2 + (3c+b-3)^2 + 7$. □

Propositions 4 and 5 tell us that the MIXMAX-$(m, k, d, c)$ has a bad structure when $c$ is small, and the MIXMAX-$(m, k, d, c, b)$ has a bad structure when both $c$ and $b$ are close to 0, respectively. The next proposition emphasizes the fact that a large value of $c$ is also not sufficient to guarantee good quality. It shows that if the modulus $m$ is near a small multiple of $c$, there is also a bad structure.

**Proposition 6** *For the MIXMAX-$(m, k, d, c)$ generator with $c \geq 1$, suppose $m = qc + r$ where $q > 0$ and $|r|$ are small integers ($r$ can be negative).*

*If $k \geq 6$, $0 \leq j \leq k-6$, and $\{4+j, 5+j, k+3+j, k+4+j, k+5+j\} \subseteq I$, then there is a set of $5q + |q+r| - 1$ equidistant parallel hyperplanes that contain all the points of $\Psi_s(I)$. These hyperplanes are at distance $1/\ell$ apart, where $\ell^2 = 7q^2 + (q+r)^2$.*

*Under the stronger conditions that $k \geq 7$, $0 \leq j \leq k-7$, and $\{4+j, 5+j, 6+j, k+3+j, k+4+j, k+5+j, k+6+j\} \subseteq I$, $\Psi_s(I)$ is covered by another family of equidistant parallel hyperplanes at distance $1/\ell$ apart, where $\ell^2 = 5q^2 + r^2 + (q+r)^2$. This last bound is smaller than the bound in the first part if and only if $2q^2 > r^2$.*

*In both cases, if $d = 0$, one can also take $j = -1$ and reduce the lower bound on $k$ by 1.*

**Proof.** For the first part, take

$$\begin{aligned}
\mathbf{w} &= q(\mathbf{w}_{k+4+j} - 2\mathbf{w}_{k+5+j} + \mathbf{w}_{k+6+j}) \bmod m \\
&= q(0, \ldots, 0, 1-c, -1, 0, \ldots, 0, 1, -2, 1, 0, \ldots) \bmod m \\
&= (0, \ldots, 0, q+r, -q, 0, \ldots, 0, q, -2q, q, 0, \ldots),
\end{aligned}$$

in which the $q+r$ is at position $5+j$ and the $-2q$ is at position $k+5+j$. Thus we have the relationship $((q+r)u_{4+j} - qu_{5+j} + qu_{k+3+j} - 2qu_{k+4+j} + qu_{k+5+j}) \bmod 1 = 0$. So if $I$

satisfies the condition, we have a dual vector whose $L^1$ length at most $5q+|q+r|$ and squared Euclidean length $7q^2+(q+r)^2$.

For the second part, we have

$$\begin{aligned}\mathbf{w} &= q(\mathbf{w}_{k+4+j} - \mathbf{w}_{k+5+j} - \mathbf{w}_{k+6+j} + \mathbf{w}_{k+7+j}) \bmod m \\ &= q(0,\dots,0,1-c,-c,-1,0,\dots,0,1,-1,-1,1,0,\dots) \bmod m \\ &= (0,\dots,0,q+r,r,-q,0,\dots,0,q,-q,-q,q,0,\dots),\end{aligned}$$

in which the $q+r$ is at position $5+j$ and the first $q$ is at position $k+4+j$. If $I$ satisfies the condition in the first part, we have a vector in the dual of $L_s(I)$ whose only nonzero coordinates correspond to the nonzero coordinates of $\mathbf{w}$. This vector has $L^1$ length of $5q+|r|+|q+r|$ and squared Euclidean length $5q^2+r^2+(q+r)^2$.

When $d=0$, one can easily verify that this development also works for $j=-1$. □

We have seen so far that the MIXMAX always produces a bad lattice structure if we keep the first two coordinates of each vector. If we skip these two coordinates, there is still always a bad lattice structure for the MIXMAX-$(m,k,d)$, as seen in Proposition 3, and for the MIXMAX with four or five parameters, the lattice structure is always bad if the parameters $c$ and $b$ are too small. Moreover, even if $c$ is large and we skip the first three values of each vector, there are situations where the lattice structure is also very bad, depending on the choices of parameters $c$ and $b$. In other situations, the lattice structure can be explored by applying the spectral test numerically to specific MIXMAX instances.

# 5. Application to some proposed MIXMAX generators

We now apply our results to specific MIXMAX generators proposed by Savvidy (2017).

**Example 1** Consider the small MIXMAX-$(m,k,d,c)$ proposed in the MIXMAX implementation of Savvidy (2017), for which $m=2^{61}-1$, $k=8$, $d=0$, and $c=2^{53}+1$. With this $c$, the matrix $\mathbf{A}$ has many large entries, which does not occur for the MIXMAX-$(m,k,d)$, so one might have hoped for a good lattice structure if we skip some coordinates. But here, $m=256c-257$, and Proposition 6 applies with $q=256$ and $r=-257$.

The first part of the proposition (with $j=0$) says for example that for $I=\{4,5,11,12,13\}$, $\Psi_s(I)$ is contained in at most $5q+|q+r|-1=1280$ equidistant parallel hyperplanes at distance $1/\ell$ apart, where $\ell^2=7q^2+(q+r)^2=458753$, i.e., $\ell\approx 677.313$, for $s=5$. By

applying the spectral test numerically, we found that this $\ell$ is also the exact length $\ell_s(I)$ of the shortest vector for this particular $I$ (and also for $I' = \{0, 1, \ldots, 13\}$), and it gives $S_s(I) \approx 2.3859 \times 10^{-16}$, which is extremely small (a good value should be close to 1, and certainly not less than say 0.1).

The second part of the proposition tells us that for $I = \{4, 5, 6, 11, 12, 13, 14\}$, the points of $\Psi_s(I)$ are also all covered by another family of equidistant parallel hyperplanes at distance $1/\ell$ apart, where $\ell^2 = 5q^2 + r^2 + (q+r)^2 = 393730$, i.e., $\ell \approx 627.479$, in $s = 7$ dimensions. This $\ell$ is also the exact length $\ell_s(I)$ of the shortest vector for this $I$ (and also for $I' = \{0, 1, \ldots, 14\}$). The corresponding normalized figure of merit is $S_s(I) \approx 2.0219 \times 10^{-16}$.

Note that these bad projections show up even if we skip the first three coordinates of each vector, since $I$ never involves these coordinates. If we do not skip the first two coordinates of each vector, Proposition 1 applies and the situation is much worse.

**Example 2** This MIXMAX-$(m, k, d, c)$ example was also proposed (and highly recommended) by Savvidy (2017). It has $m = 2^{61} - 1$, $k = 240$, $d = 487013230256099140$, and $c = 2^{51} + 1$. Here we have $m = 1024c - 1025$, so Proposition 6 applies as in the previous example, this time with $q = 1024$ and $r = -1025$.

The proposition tells us that for $I = \{4, 5, 243, 244, 245\}$, $\Psi_s(I)$ is contained in at most $5q + |q + r| - 1 = 5120$ equidistant parallel hyperplanes at distance $1/\ell$ apart, where $\ell^2 = 7q^2 + (q + r)^2 = 7340033$, i.e., $\ell \approx 2709.245$, for $s = 5$. This $\ell$ turns out to be the exact length of the shortest vector for this $I$. The corresponding normalized figure of merit is $S_s(I) \approx 9.5436 \times 10^{-16}$.

For the larger index set $I = \{4, 5, 6, 243, 244, 245, 246\}$, the points of $\Psi_s(I)$ all belong to another family of parallel hyperplanes at distance $1/\ell$ apart, where $\ell^2 = 5q^2 + r^2 + (q+r)^2 = 6293506$, i.e., $\ell \approx 2508.686$, in $s = 7$ dimensions. This $\ell$ is again the length of the shortest vector for this $I$ and we have $S_s(I) \approx 8.0836 \times 10^{-16}$, which is again very small. This means that the distance between successive hyperplanes that contain all the points is much larger than what one should expect with $m = 2^{61} - 1$ in 7 dimensions. Note that the choices of $d$ and $k$ have no impact on these results: the upper bound on $\ell_s(I)$ that we obtained remains the same if we change $d$ or $k$, as long as $k \geq 7$.

As in the previous example, these projections appear even if we skip the first three coordinates, and if we keep the first two coordinates then Proposition 1 applies.

# 6. Conclusion

We have examined the lattice structure of the vectors (or points) of successive output values produced by the MIXMAX generator. We showed that the projections of those points over certain subsets of coordinates have a very bad structure, in which all the points belong to a relatively small number of parallel hyperplanes, much smaller than what one would expect given the size of the modulus. One can get rid of these very bad structures in the output by skipping some output values, but we saw that other structures then show up, due to linear relationships between other subsets of coordinates. These relationships come from the special structure of the matrix $\mathbf{A}$. One can alleviate this weak behavior by skipping more coordinates in the output vectors (those that are involved in the bad linear relationships), but this slows down the generator.

What is the practical impact of these bad structures on simulation results if we do not skip coordinates, or if we skip just a few? For some applications there may be no visible impact, but for other applications the poor structures may introduce significant bias if there is some kind of alignment or synergistic effect between the poor lattice structure and the way the random numbers are used in the application. This type of effect is not easy to predict in general, but it has been observed in the past for RNGs that have a poor lattice structure similar to the one that we have unveiled here; see Ferrenberg et al. (1992) and Tezuka et al. (1993), for example. Therefore, we think it is important for the MIXMAX users to be aware of these structural properties and be cautious about them.

# Acknowledgments

P. L'Ecuyer wants to thank G. K. Savvidy for inviting him to the MIXMAX Network Meeting at the CERN, in Geneva, in July 2016, which triggered his interest in the MIXMAX generator. This work has been supported by an NSERC-Canada Discovery Grant, a Canada Research Chair, and an Inria International Chair (in Rennes, France) to P. L'Ecuyer.

# References

Afflerbach, L., H. Grothe. 1988. The lattice structure of pseudo-random vectors generated by matrix generators. *Journal of Computational and Applied Mathematics* **23** 127–131.

Akopov, N. Z., G. K. Savvidy, N. G. Ter-Arutyuntan Savvidy. 1991. Matrix generators for pseudorandom numbers. *Journal of Computational Physics* **97** 573–579.

Conway, J. H., N. J. A. Sloane. 1999. *Sphere Packings, Lattices and Groups*. 3rd ed. Grundlehren der Mathematischen Wissenschaften 290, Springer-Verlag, New York.

Couture, R., P. L'Ecuyer. 1994. On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. *Mathematics of Computation* **62** 798–808.

Couture, R., P. L'Ecuyer. 1996. Orbits and lattices for linear random number generators with composite moduli. *Mathematics of Computation* **65** 189–201.

Coveyou, R. R., R. D. MacPherson. 1967. Fourier analysis of uniform random number generators. *Journal of the ACM* **14** 100–119.

Ferrenberg, A. M., D. P. Landau, Y. J. Wong. 1992. Monte Carlo simulations: Hidden errors from "good" random number generators. *Physical Review Letters* **69** 3382–3384.

Fincke, U., M. Pohst. 1985. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation* **44** 463–471.

Grothe, H. 1988. Matrixgeneratoren zur Erzeugung gleichverteilter Pseudozufallsvektoren. Dissertation (thesis), Tech. Hochschule Darmstadt, Germany.

Knuth, D. E. 1998. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. 3rd ed. Addison-Wesley, Reading, MA.

L'Ecuyer, P. 1990. Random numbers for simulation. *Communications of the ACM* **33** 85–97.

L'Ecuyer, P. 1994. Uniform random number generation. *Annals of Operations Research* **53** 77–120.

L'Ecuyer, P. 1999. Tables of linear congruential generators of different sizes and good lattice structure. *Mathematics of Computation* **68** 249–260. See the Errata at `http://www.iro.umontreal.ca/~lecuyer/myftp/papers/latrules99Errata.pdf`.

L'Ecuyer, P. 2006. Uniform random number generation. S. G. Henderson, B. L. Nelson, eds., *Simulation*. Handbooks in Operations Research and Management Science, Elsevier, Amsterdam, The Netherlands, 55–81. Chapter 3.

L'Ecuyer, P. 2012. Random number generation. J. E. Gentle, W. Haerdle, Y. Mori, eds., *Handbook of Computational Statistics*, 2nd ed. Springer-Verlag, Berlin, 35–71.

L'Ecuyer, P. 2017. History of uniform random number generation. *Proceedings of the 2017 Winter Simulation Conference*. IEEE Press. Forthcoming.

L'Ecuyer, P., R. Couture. 1997. An implementation of the lattice and spectral tests for multiple recursive linear random number generators. *INFORMS Journal on Computing* **9** 206–217.

L'Ecuyer, P., D. Munger, B. Oreshkin, R. Simard. 2017. Random numbers for parallel computers: Requirements and methods, with emphasis on GPUs. *Mathematics and Computers in Simulation* **135** 3–17. Open access at `http://dx.doi.org/10.1016/j.matcom.2016.05.005`.

L'Ecuyer, P., R. Simard. 2014. On the lattice structure of a special class of multiple recursive random number generators. *INFORMS Journal on Computing* **26** 449–460.

Marsaglia, G. 1968. Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences of the United States of America* **60** 25–28.

Marsaglia, G., A. Zaman. 1991. A new class of random number generators. *The Annals of Applied Probability* **1** 462–480.

Niederreiter, H. 1986. A pseudorandom vector generator based on finite field arithmetic. *Mathematica Japonica* **31** 759–774.

Savvidy, G. K., N. G. Ter-Arutyuntan-Savvidy. 1991. On the Monte Carlo simulation of physical systems. *Journal of Computational Physics* **97** 566–572.

Savvidy, K. G. 2015. The MIXMAX random number generator. *Computer Physics Communications* **196** 161–165.

Savvidy, K. G. 2017. MIXMAX manual. See `https://www.hepforge.org/archive/mixmax/MANUAL.pdf`.

Savvidy, K. G., G. K. Savvidy. 2016. Spectrum and entropy of C-systems MIXMAX random number generator. *Chaos, Solitons and Fractals* **91** 33–38.

Tahmi, E.-H. A. D. E. 1982. Contribution aux générateurs de valeurs aléatoires. Dissertation (thesis), Université des Sciences et Technologies Houari Boumédienne.

Tezuka, S., P. L'Ecuyer, R. Couture. 1993. On the add-with-carry and subtract-with-borrow random number generators. *ACM Transactions of Modeling and Computer Simulation* **3** 315–331.