ORBITS AND LATTICES FOR LINEAR RANDOM NUMBER GENERATORS WITH COMPOSITE MODULI

RAYMOND COUTURE AND PIERRE L'ECUYER

ABSTRACT. In order to analyze certain types of combinations of multiple recursive linear congruential generators (MRGs), we introduce a generalized spectral test. We show how to apply the test in large dimensions by a recursive procedure based on the fact that such combinations are subgenerators of other MRGs with composite moduli. We illustrate this with the well-known RANMAR generator. We also design an algorithm generalizing the procedure to arbitrary random number generators.

1. INTRODUCTION

The structure of a (uniform) random number generator generally consists of a finite *state* space Σ, together with a *transition* mapping

$$T : \Sigma \to \Sigma$$

determining the evolution of the system, and an *output* mapping

$$\Phi : \Sigma \to \mathbf{Q}/\mathbf{Z}.$$

Starting from an arbitrary *seed* $\sigma_0 \in \Sigma$, this generator produces a sequence

$$\Phi(T^i(\sigma_0)) \in \mathbf{Q}/\mathbf{Z}, \quad i = 0, 1, \ldots$$

of *pseudorandom numbers*. One can associate to such a system (Σ, T, Φ), and each positive integer d, a *lattice* Λ_d in $\mathbf{R}^d$ as follows. First, we define the mapping $\Phi^{(d)} : \Sigma \to (\mathbf{R}/\mathbf{Z})^d$ by

$$\Phi^{(d)}(\sigma) = (\Phi(\sigma), \Phi(T(\sigma)), \ldots, \Phi(T^{d-1}(\sigma))).$$

We then define $\Lambda_d \subset \mathbf{R}^d$ as the inverse image, by the canonical mapping

$$\text{can} : \mathbf{R}^d \to (\mathbf{R}/\mathbf{Z})^d, \qquad (1)$$

of the subgroup of $(\mathbf{R}/\mathbf{Z})^d$ generated by all differences between any two elements of $\Phi^{(d)}(\Sigma)$. The structure of the lattice Λ_d is indicative of the distribution of the set of all (overlapping) d-tuples of successive values of the generator. Determining

1991 *Mathematics Subject Classification.* 65C10.

Key words and phrases. Random number generation, lattice structure, combined generators.

This work has been supported by NSERC-Canada grant # OGP0110050 and FCAR-Québec grant # 93ER1654 to the second author.

the length of the shortest vector of the *dual* lattice $\Lambda^{(d)}$ to Λ_d, the so-called *spectral test*, gives significant insight into this structure and the distribution properties of the corresponding generator [3, 5, 8].

However, if the action of T on Σ is not transitive, that is, if there exists some T-invariant, proper subset $\Sigma' \subset \Sigma$, such a subset also defines a (sub)generator $(\Sigma', T|_{\Sigma'}, \Phi|_{\Sigma'})$, and one can, as above, consider its associated lattices Λ_d. These will be contained, strictly in general, in the corresponding lattices defined by Σ. The question of the relative significance of the various lattices arises. In particular, if T is not one-to-one, then $T(\Sigma), T^2(\Sigma), \ldots$ is a decreasing sequence of T-invariant subsets, ending with $\cap_i T^i(\Sigma)$, which is especially interesting, since it is precisely the set Σ^{r} of *recurrent* states. If this set quickly attracts into it an arbitrary state, then the lattices associated with Σ^{r} are more relevant to the behavior of the generator than those associated with Σ.

We will discuss this question for the class, defined in Section 3, of multiple recursive linear congruential random number generators (MRGs) with respect to an arbitrary modulus. As the linear generators considered are not assumed homogeneous, we show in Section 2 how their study can be reduced to that of corresponding homogeneous generators. Combination, as defined in Section 4, is a standard construction in the design of random number generators [6, 12]. Although, the combination of MRGs is, in general, not a MRG, it is shown there that, in case of relatively prime moduli, it is a subgenerator of another MRG with modulus equal to the product of the component moduli, and which we will call their *product* MRG. One can then study the combined generator through this MRG since, in general, for any subgenerator of an MRG, there is a simple way to take advantage, in the task of determining the short vectors in $\Lambda^{(d)}$, of the solution of the corresponding lower dimensional problem (see [5, 8] for the case of LCGs). This is generalized to the case of arbitrary generators by means of the algorithms described in Section 7. We illustrate, in Section 6, our discussion with a well known generator proposed by Marsaglia, Zaman, and Tsang [10], usually designated by RANMAR. Some general principles, which indicate a precise limitation on the possible improvement obtained using combination, are applied to determine, in this instance, a shortest vector in $\Lambda^{(d)}$ for d up to 100.

We will use the following terminology. An *isomorphism* between the two generators (Σ_1, T_1, Φ_1) and (Σ_2, T_2, Φ_2) is a one-to-one mapping $f : \Sigma_1 \simeq \Sigma_2$ such that $T_2 \circ f = f \circ T_1$, and $\Phi_1 = \Phi_2 \circ f$. All properties of interest to us are invariant under such an isomorphism. For instance, the associated lattices Λ_d are identical. If the state spaces have the additional structure of an abelian group, we will say that the isomorphism is *additive* if it preserves the group law. We recall that the *volume* of a lattice is the volume of the parallelipiped generated by one of its bases. For a vector $v \in \mathbf{R}^d$ we denote by $v^\sim$ the vector in $\mathbf{R}^{d+1}$ obtained from v by adding a zero coordinate. We will denote by e_i, $i = 1, \ldots, d$, the canonical basis for $\mathbf{R}^d$ —so that $e_i^\sim = e_i$!— and by S the (linear) right-shift on $\mathbf{R}^d$ defined by $S(e_i) = e_{i+1}$, $i = 1, \ldots, d-1$, and $S(e_d) = 0$.

2. Additive generators

We will say that a generator (Σ, T, Φ) is *additive* if its state space Σ has the additional structure of an abelian group (we will write its law additively), and if the transformation

$$T_0 : \Sigma \to \Sigma$$

defined by $T_0(\sigma) = T(\sigma) - T(0)$, as well as the output mapping Φ, is a group homomorphism. The generator (Σ, T_0, Φ) is the corresponding *homogeneous* generator (also additive), and we refer to $T(0)$ as the *increment.* More generally, if $\Sigma' \subset \Sigma$ is T-invariant (though not necessarily a subgroup), and therefore defining a subgenerator, then the subgroup Σ'_0 generated by the set of differences $\sigma_1 - \sigma_2$ with $\sigma_1, \sigma_2 \in \Sigma'$, is T_0-invariant and defines a corresponding *homogeneous* subgenerator (that is, a subgenerator of (Σ, T_0, Φ) given by a subgroup of Σ). It will be seen, in this section, how the study of an additive generator, and its subgenerators, with their associated lattices, is reduced to the homogeneous case. Homogeneous subgenerators will be characterised algebraically in Section 5.

Example 1. The set Σ^{r} of recurrent states of an additive generator (Σ, T, Φ) is obviously T-invariant, and the corresponding homogeneous subgenerator is defined by the subgroup Σ_0^{r} of recurrent states with respect to T_0. Indeed, if $\sigma_1, \sigma_2 \in \Sigma^{\mathrm{r}}$ and n is a common multiple of their periods, then $T_0^n(\sigma_1 - \sigma_2) = T^n(\sigma_1) - T^n(\sigma_2) = \sigma_1 - \sigma_2$, so $\sigma_1 - \sigma_2 \in \Sigma_0^{\mathrm{r}}$. Conversely, if $\sigma \in \Sigma_0^{\mathrm{r}}$ and $\sigma_2 \in \Sigma^{\mathrm{r}}$, then $T^n(\sigma + \sigma_2) = T_0^n(\sigma) + T^n(\sigma_2)$, and this is $\sigma + \sigma_2$ if n is a common multiple of the periods of σ and σ_2 (relative to T_0 and T, respectively). We thus obtain $\sigma + \sigma_2 \in \Sigma_0^{\mathrm{r}}$.

Consider the mapping (not necessarily one-to-one) $T_\Delta : \Sigma \to \Sigma$ defined by $T_\Delta(\sigma) = T(\sigma) - \sigma$. Then, clearly

$$T_\Delta(\Sigma') \subset \Sigma'_0. \tag{2}$$

Lemma 1. *The mapping T_Δ transforms T into T_0, that is, we have*

$$T_\Delta \circ T = T_0 \circ T_\Delta.$$

Proof. For $\sigma \in \Sigma$ we have $T_\Delta \circ T(\sigma) = T^2(\sigma) - T(\sigma) = T_0 \circ T(\sigma) - T_0(\sigma) = T_0 \circ T_\Delta(\sigma)$. $\square$

Example 2. If Σ' is the forward T-orbit of σ_0 then, by Lemma 1, $T_\Delta(\Sigma')$ is the forward T_0-orbit of $T_\Delta(\sigma_0)$. Therefore, in this case, Σ'_0 is equal to the subgroup generated by $T_\Delta(\Sigma')$ since it is, from its definition, generated by the differences $(T^n(\sigma_0) - T^{n-1}(\sigma_0)) = T_0^{n-1}(T_\Delta(\sigma_0))$.

In general, not every homogeneous subgenerator arises in this way as a Σ'_0 for some T-invariant subset Σ'. We have

Proposition 1. *A T_0-invariant subgroup of Σ is of the form Σ'_0 for some T-invariant subset Σ' of Σ if and only if it has a non-void intersection with $T_\Delta(\Sigma)$.*

Proof. By (2), the condition is clearly necessary. Conversely, assume Σ_1 is a T_0-invariant subgroup and that $T_\Delta(\sigma') \in \Sigma_1$. Put $\Sigma' = \sigma' + \Sigma_1$. Then Σ' is T-invariant since $T(\sigma' + \sigma_1) = \sigma' + T_\Delta(\sigma') + T_0(\sigma_1) \in \Sigma'$ for $\sigma_1 \in \Sigma_1$ and $\Sigma'_0 = \Sigma_1$. $\square$

If, for instance, T is a translation, so that $T_\Delta \equiv T(0)$, then the condition on the T_0-invariant subgroup is that it should contain $T(0)$, that is, it should also be T-invariant.

We define $\Phi_0^{(d)} : \Sigma \to (\mathbf{R}/\mathbf{Z})^d$ by

$$\Phi_0^{(d)}(\sigma) = (\Phi(\sigma), \Phi(T_0(\sigma)), \ldots, \Phi(T_0^{d-1}(\sigma))).$$

Proposition 2. *A subgenerator of an additive generator, and its corresponding homogeneous subgenerator, have identical associated lattices Λ_d and $\Lambda^{(d)}$. The volume of $\Lambda^{(d)}$ is given by the order of the image, by $\Phi_0^{(d)}$, of the state space of the homogeneous subgenerator.*

Proof. For any T-invariant subset Σ', $\Phi_0^{(d)}(\Sigma'_0)$ is the subgroup generated by all differences of pairs of elements of $\Phi^{(d)}(\Sigma')$, and the first statement follows. The order of $\Phi_0^{(d)}(\Sigma'_0)$ is equal to the index $[\Lambda_d : \mathbf{Z}^d]$ which is equal to the reciprocal of the volume of Λ_d. It is thus equal to the volume of $\Lambda^{(d)}$. □

Example 3. Assume that T is a translation and that $\Phi(\Sigma)$ has exponent m. Then $\Phi_0^{(d)}(\Sigma)$ is the subgroup of elements of $((1/m)\mathbf{Z}/\mathbf{Z})^d$ with identical coordinates. The lattice Λ_d is therefore the set of vectors $1/m \sum_i x_i e_i$ with integral x_i such that $x_i \equiv x_j \pmod{m}$, and its dual $\Lambda^{(d)}$ is the set of vectors $\sum_i x_i e_i$ with integral x_i such that $\sum_i x_i \equiv 0 \pmod{m}$.

3. Multiple recursive linear congruential generators

We now consider a special class of additive generators, namely the multiple recursive (inhomogeneous) linear congruential generators (MRG for short) which can be defined as follows. Call a group an *f-group* if it is finite, abelian and, m being its exponent, if it admits a basis as a $\mathbf{Z}/m\mathbf{Z}$-module.

Definition 1. An additive generator (Σ, T, Φ) is called an MRG if the state space Σ is an f-group and the output mapping Φ is *generic* in the sense that its kernel contains no non-zero forward T_0-orbit.

The *modulus* (resp. *order*) of a given MRG, (Σ, T, Φ), is the exponent (resp. rank) of Σ. If m is the modulus and k the order, then the mapping $\Phi_0^{(k)}$ is one to one with image $\Phi_0^{(k)}(\Sigma) = ((1/m)\mathbf{Z}/\mathbf{Z})^k$. Therefore, there exists a state $\mu \in \Sigma$, uniquely determined by the conditions

$$\Phi(T_0^{i-1}(\mu)) = (1/m)\,\delta_{ik}, \quad i = 1, \ldots, k. \tag{3}$$

We refer to μ as the *canonical unit* of the MRG. We also refer to the (monic) characteristic polynomial $P_{\mathrm{ch}}(X) \in \mathbf{Z}/m\mathbf{Z}[X]$ of T_0 as the characteristic polynomial of the generaror. Clearly, a $\mathbf{Z}/m\mathbf{Z}$-basis for Σ is given by $\mu, T_0(\mu), \ldots, T_0^{k-1}(\mu)$.

Proposition 3. *For an MRG (Σ, T, Φ) with modulus m and characteristic polynomial $P_{\mathrm{ch}}(X)$, the following conditions on $P(X) \in \mathbf{Z}/m\mathbf{Z}[X]$, are equivalent.*

i) $P(T_0)(\mu) = 0$,
ii) $P(T_0) = 0$,
iii) $P_{\mathrm{ch}}(X)$ *divides* $P(X)$.

In particular $P_{\mathrm{ch}}(X)$ is also the minimal polynomial of T_0.

Proof. We have $P_{\text{ch}}(T_0) = 0$ by the Hamilton-Cayley theorem. If $P_{\text{ch}}(X)$ divides $P(X)$ then clearly $P(T_0) = 0$, and $P(T_0)(\mu) = 0$. Assume, conversely, that $P(T_0)(\mu) = 0$. Then $P(T_0) = 0$ since an arbitrary element $\sigma \in \Sigma$ can be expressed as $\sigma = P_1(T_0)(\mu)$ for some $P_1(X) \in \mathbf{Z}/m\mathbf{Z}[X]$, and $P(T_0)(\sigma) = P_1(T_0)P(T_0)(\mu) = 0$. The Euclidean algorithm provides us with polynomials $Q(X), R(X) \in \mathbf{Z}/m\mathbf{Z}[X]$ such that $R(X)$ has degree less than the order, and $P(X) = P_{\text{ch}}(X)Q(X) + R(X)$. It follows that $R(T_0)(\mu) = 0$, so that $R(X) = 0$, and $P_{\text{ch}}(X)$ divides $P(X)$. □

Proposition 4. *Two additively isomorphic MRGs have the same modulus and characteristic polynomial. Further, there is at most one additive isomorphism between them and their canonical units correspond under it. A homogeneous MRG is determined up to an additive isomorphism by its modulus and its characteristic polynomial.*

Proof. Consider the MRGs (Σ_1, T_1, Φ_1) and (Σ_2, T_2, Φ_2), with respective canonical units μ_1 and μ_2. Assume there is an additive isomorphism $f : \Sigma_1 \to \Sigma_2$ between them. Clearly Σ_1 and Σ_2 then have the same exponent. We also have $T_2 \circ f = f \circ T_1$ so that $T_2(0) = f(T_1(0))$, and

$$T_{2,0} \circ f = f \circ T_{1,0}. \tag{4}$$

The first statement in the proposition follows. Since $\Phi_2 \circ f = \Phi_1$, we obtain, using (4), $\Phi_{2,0}^{(k)} \circ f = \Phi_{1,0}^{(k)}$, k being the order. It follows that $f(\mu_1) = \mu_2$ and, again using (4), that $f(T_{1,0}^i(\mu_1)) = T_{2,0}^i(\mu_2)$ for $1 \leq i < k$. The second statement follows. Assume now that the two generators are homogeneous with the same modulus m and same characteristic polynomial $P_{\text{ch}}(X)$. Since, by Proposition 3, we have for $P(X) \in \mathbf{Z}/m\mathbf{Z}[X]$, that $P(T_1)(\mu_1) = 0$ (resp. $P(T_2)(\mu_2) = 0$) if and only if $P_{\text{ch}}(X)|P(X)$, the correspondence $P(T_1)(\mu_1) \mapsto P(T_2)(\mu_2)$ is well defined, and is the required isomorphism between the two generators. □

If we lift the characteristic polynomial $P_{\text{ch}}(X)$ of an MRG (Σ, T, Φ) to a monic polynomial $X^k - a_1X^{k-1} - \ldots - a_k \in \mathbf{Z}[X]$, and put $b = \Phi(T^k(0) - a_1T^{k-1}(0) - \cdots - a_kT^0(0))$, the output sequence $u_i = \Phi(T^i(\sigma_0)) \in \mathbf{Q}/\mathbf{Z}$, $i = 0, 1, \ldots$ will satisfy the recurrence

$$u_i = a_1u_{i-1} + \cdots + a_ku_{i-k} + b, \quad i \geq k.$$

In fact, u_i and b belong to $(1/m)\mathbf{Z}/\mathbf{Z}$ if m is the modulus of the MRG, and our generator is essentially identical to a multiple recursive (inhomogeneous) linear congruential generator—as defined, for instance, in [3, 6, 7, 11]—for the (arbitrary) modulus m.

It follows from Propositions 2 and 4 that the lattices Λ_d and $\Lambda^{(d)}$ associated with an MRG are determined by its modulus and characteristic polynomial. In particular, if we put, for $d > k$,

$$w_{\text{ch}} = -a_ke_1 - \cdots - a_1e_k + e_{k+1}, \tag{5}$$

we have the following.

Proposition 5. *If $d \leq k$ then $\Lambda^{(d)} = m\mathbf{Z}^d$. If $d > k$, then $\Lambda^{(d)}$ admits the lattice basis $me_1, \ldots, me_k, w_{\text{ch}}, Sw_{\text{ch}}, \ldots, S^{d-k-1}w_{\text{ch}}$.*

Proof. Since Φ is generic, $\Phi_0^{(d)}(\Sigma)$ is the subgroup $((1/m)\mathbf{Z}/\mathbf{Z})^d$ when $d \leq k$, and has order equal to m^k for $d \geq k$. The first statement follows. Assume $d > k$. By Proposition 2, $\Lambda^{(d)}$ has volume equal to m^k and, since the proposed vectors clearly belong to $\Lambda^{(d)}$ and generate a lattice also of volume m^k, this lattice must be $\Lambda^{(d)}$. $\square$

4. Products and extensions of MRGs

From a given finite family of generators (Σ_i, T_i, Φ_i) one may form the *combined generator* $(\prod_i \Sigma_i, \prod_i T_i, \Phi)$ where $\Phi((\sigma_i)_i) = \sum_i \Phi_i(\sigma_i)$. (Other combination methods have been used in actual implementations [1, 6, 9] but they are often well approximated by combinations in the above sense.) The lattices Λ_d (resp. $\Lambda^{(d)}$) associated with a combination are the sum (resp. intersection) of those associated with the components.

The combination of MRGs of the same order, and with pairwise relatively prime moduli, is again an MRG. Its modulus m is the product of the component moduli m_i and its characteristic polynomial $P_{\mathrm{ch}}(X)$ is determined by the conditions $P_{\mathrm{ch}}(X) \equiv P_{\mathrm{ch},i}(X) \pmod{m_i}$ where $P_{\mathrm{ch},i}(X)$ are the component characteristic polynomials. More generally, if the orders k_i are not all equal, it would seem natural to consider an MRG of order $\bar{k} = \max_i k_i$ with a characteristic polynomial $P_{\mathrm{ch}}(X)$ satisfying $P_{\mathrm{ch}}(X) \equiv X^{\bar{k}-k_i} P_{\mathrm{ch},i}(X) \pmod{m_i}$. However, the state space of such an MRG has a cardinality larger than that of the combined generator, and the question arises of determining the exact relation between these two generators. This can be done by introducing the notion of a *nil-extension* of MRGs.

An *extension* of a given generator (Σ, T, Φ) is a generator $(\bar{\Sigma}, \bar{T}, \bar{\Phi})$ with $\Sigma \subset \bar{\Sigma}$, and such that $T = \bar{T}$ and $\Phi = \bar{\Phi}$ over Σ. When both generators are additive, we will say that the extension is *additive* if Σ is a subgroup of $\bar{\Sigma}$. The increments $T(0)$ and $\bar{T}(0)$ are then equal and contained in Σ. In case of two MRGs with equal moduli, an extension will be called a *nil-extension* if it is additive and if any $\bar{T}_0$-orbit in $\bar{\Sigma}$ eventually ends up in Σ.

Lemma 2. *Assume that $(\bar{\Sigma}, \bar{T}, \bar{\Phi})$ is a nil-extension of (Σ, T, Φ). Let $\bar{k}$, $\bar{P}_{\mathrm{ch}}(X)$, $\bar{\mu}$ and k, $P_{\mathrm{ch}}(X)$, μ be their respective order, characteristic polynomial and canonical unit. If the integer i is sufficiently large, so that $\bar{T}_0^i(\bar{\Sigma}) \subset \Sigma$, then $i \geq \bar{k} - k$. If $\bar{T}_0^{\bar{k}-k}(\bar{\Sigma}) \subset \Sigma$, then $\bar{P}_{\mathrm{ch}}(X) = X^{\bar{k}-k} P_{\mathrm{ch}}(X)$, and $\bar{T}_0^{\bar{k}-k}(\bar{\mu}) = \mu$.*

Proof. Assume $\bar{T}_0^i(\bar{\Sigma}) \subset \Sigma$ with $i < \bar{k} - k$. Then $\bar{T}_0^i(\bar{\mu}) \in \Sigma$ is not 0, but $\Phi(T_0^{i+j}(\bar{\mu})) = 0$ for $0 \leq j < k$, contradicting the genericity of Φ.

If $\bar{T}_0^{\bar{k}-k}(\bar{\Sigma}) \subset \Sigma$ then, by Proposition 3, we have $\bar{P}_{\mathrm{ch}}(X) \mid X^{\bar{k}-k} P_{\mathrm{ch}}(X)$. Since the two polynomials are monic and of the same degree, they are equal. To prove the last statement it is sufficient to remark that $\bar{T}_0^{\bar{k}-k}(\bar{\mu}) \in \Sigma$ satisfies the conditions (3) defining μ. $\square$

If a nil-extension satisfies (with the above notations) $\bar{T}_0^{\bar{k}-k}(\bar{\Sigma}) \subset \Sigma$, we will say it is *minimal.*

Proposition 6. *An MRG of order k admits a unique (up to an additive isomorphism) minimal nil-extension of order k' for each integer $k' > k$.*

Proof. Let (Σ, T, Φ) be the given generator, m its modulus and μ its canonical unit. Embed Σ as a direct factor in an f-group $\bar{\Sigma}$ of rank $\bar{k}$ and exponent m. Choose a supplement $\Sigma' \subset \bar{\Sigma}$ to Σ (so that $\bar{\Sigma} = \Sigma \oplus \Sigma'$), and choose a $\mathbf{Z}/m\mathbf{Z}$-basis, $\mu_1, \ldots, \mu_{\bar{k}-k}$ for Σ'. Define $\bar{T} : \bar{\Sigma} \to \bar{\Sigma}$ so that its restriction to Σ is equal to T, and such that $\bar{T}_0$ is an homomorphism satisfying the conditions $\bar{T}_0(\mu_i) = \mu_{i+1}$, $i = 1, \ldots, \bar{k} - k - 1$, and $\bar{T}_0(\mu_{\bar{k}-k}) = \mu$. Define $\bar{\Phi}$ to be equal to Φ on Σ, and 0 on Σ'. $(\bar{\Sigma}, \bar{T}, \bar{\Phi})$ is the required extension. Two nil-extensions of the same order are (additively) isomorphic by Proposition 4 and the preceding lemma. $\square$

We can now define the *product* MRG of a finite family of MRGs (Σ_i, T_i, Φ_i) of possibly distinct orders k_i, and with pairwise relatively prime moduli, as the combination of their nil-extensions of order $\bar{k} = \max_i k_i$. This product is an additive extension of the combined generator, and is determined up to an additive isomorphism. Any orbit in the product is eventually absorbed by the combination so that the two generators have the same set of recurrent states, namely $\prod_i \Sigma_i^{\mathrm{r}}$.

5. A ring structure for MRGs

One can introduce a ring structure in several ways in the state space of an MRG (Σ, T, Φ) so that the action of T_0 is the same as multiplication by some fixed element of Σ. The following proposition singles out one of them, and we call it the *canonical* ring structure.

Proposition 7. *There exists a unique ring structure on the state space of an MRG (Σ, T, Φ) such that*

i) *its underlying additive structure is the given group structure of Σ,*
ii) *for a fixed $\tau \in \Sigma$, $T_0(\sigma) = \tau\sigma$ for $\sigma \in \Sigma$,*
iii) *the canonical unit μ is the unit element of Σ.*

We then have $\tau = T_0(\mu)$.

Proof. By Proposition 3, the mapping $P(X) \mapsto P(T_0)(\mu)$ induces a group isomorphism

$$\mathbf{Z}/m\mathbf{Z}[X]/(P_{\mathrm{ch}}(X)) \simeq \Sigma. \tag{6}$$

The natural ring structure of $\mathbf{Z}/m\mathbf{Z}[X]/(P_{\mathrm{ch}}(X))$, transferred to Σ via (6), satisfies the three conditions. Conversely, if Σ has such a ring structure, then $P(T_0)(\mu) = P(\tau)$ for all $P(X) \in \mathbf{Z}/m\mathbf{Z}[X]$, and (6) is therefore a ring isomorphism. $\square$

We notice that, in terms of the canonical ring structure, a T_0-invariant subgroup is the same as an ideal of Σ, while the subgroup generated by the forward T_0-orbit of some element in Σ is the principal ideal generated by this element. In view of Propositions 1 and 2 (see also Example 2), it is then of interest to have some insight into the ideal structure of our ring Σ.

Example 4. Assume that the MRG (Σ, T, Φ) has a prime power modulus $m = p^e$. Put $\mathfrak{p} = p\Sigma$. This is a principal ideal, and one has the simple filtration of Σ by the principal ideals $\mathfrak{p}^i$, $i = 1, \ldots, e-1$. Consider the canonical mapping

$$\Sigma \to \bar{\Sigma} = \Sigma/\mathfrak{p}. \tag{7}$$

Let $\bar{\tau}$ be the image of τ in $\bar{\Sigma}$. Let $\bar{P}_{\mathrm{ch}}(X) \in \mathbf{F}_p[X]$ be the polynomial obtained from $P_{\mathrm{ch}}(X)$ by reducing its coefficients modulo p, and $\bar{P}_{\mathrm{ch}}(X) = \prod_j \bar{P}_j^{e_j}(X)$ be its factorization into irreducible polynomials. Put $\bar{\mathfrak{p}}_j = (\bar{P}_j(\bar{\tau}))$, and let $\mathfrak{p}_j$ be its inverse image by (7) in Σ. The ideals $\mathfrak{p}_j$ are precisely the prime ideals (they are all, in fact, maximal) of Σ. More generally, any ideal of Σ containing $\mathfrak{p}$ is the inverse image by (7) of an ideal of $\bar{\Sigma}$ of the form $\prod_j \bar{\mathfrak{p}}_j^{e'_j}$, $0 \le e'_j \le e_j$. The set of ideals of Σ exhibited so far is still not sufficient to account for all ideals of Σ. For instance, if $m = 4$ and τ has minimal polynomial $P_0(X) = X^2$, then (τ) does not contain and is not contained in $\mathfrak{p} = (2)$. Neither is it a product of ideals containing $\mathfrak{p}$. A simple situation however arises if $\bar{P}_0(X) \in \mathbf{F}_p[X]$ is irreducible. The ideals $\mathfrak{p}^{e'}$, $e' = 1, \ldots, e-1$ are then the only proper ideals of Σ. Indeed, since $\mathfrak{p}$ is then the only maximal ideal, any element not contained in it is invertible. Let $\mathfrak{a}$ be any ideal of Σ, and $\mathfrak{p}^n$ the highest power of $\mathfrak{p}$ containing $\mathfrak{a}$. Then $\mathfrak{a}$ contains an element of the form $p^n\alpha$ with $\alpha \notin \mathfrak{p}$. Since α is then invertible, we obtain $\mathfrak{a} = \mathfrak{p}^n$.

6. Short vector search strategies

The search for short vectors in the dual lattices $\Lambda^{(d)}$ to Λ_d is often facilitated by the following facts, valid for arbitrary (combined) generators.

(a) The dual lattices associated to a generator satisfy

$$\Lambda^{(d-1)} \times \{0\} = \Lambda^{(d)} \cap (\mathbf{R}^{d-1} \times \{0\}).$$

(b) Shift invariance:

$$S(\Lambda^{(d)} \cap (\mathbf{R}^{d-1} \times \{0\})) \subset \Lambda^{(d)}.$$

(c) Let $\Lambda^{(d)}$ be associated with a combined generator, while $\Lambda_1^{(d_1)}$ and $\Lambda_2^{(d_2)}$ are associated with its components. If $P_1(X)$, $P_2(X) \in \mathbf{Z}[X]$ and if d (resp. d_1, d_2) is strictly larger than the degree of $P_1(X)P_2(X)$ (resp. $P_1(X)$, $P_2(X)$), then $P_1(S)(e_1) \in \Lambda_1^{(d_1)}$ and $P_2(S)(e_1) \in \Lambda_2^{(d_2)}$ imply that $P_1P_2(S)(e_1) \in \Lambda^{(d)}$.

If $\rho : \mathbf{R}^d \to \mathbf{R}^{d-1}$ is the projection on the first $d-1$ coordinates, then $\rho(\Lambda_d) = \Lambda_{d-1}$. If it is the projection on the last $d-1$ coordinates, we have meerely $\rho(\Lambda_d) \subset \Lambda_{d-1}$. These two properties imply (a) and (b) as their respective dual counterparts while (c) follows from (a) and (b). We notice that (c) gives a limitation on the improvement obtainable for a given random number generator by the process of combination. Indeed, short vectors in the component lattices $\Lambda_1^{(d_1)}$ and $\Lambda_2^{(d_2)}$ can be expressed respectively as $P_1(S)(e_1)$ and $P_2(S)(e_2)$, where the polynomials $P_1(X)$ and $P_2(X)$ have small coefficients. Their product $P_1(X)P_2(X)$ should then also have small coefficients, and provide a short vector $P_1P_2(S)(e_1) \in \Lambda^{(d)}$ (see the example below). Given a basis of 'short' vectors for $\Lambda^{(d-1)}$, (a) allows one to 'extend' it to a basis of $\Lambda^{(d)}$ without increasing the length of the vectors (see the next proposition). The extended basis can be given explicitly in case of a subgenerator of an MRG when d exceeds its order.

Proposition 8. *There exists $w \in \Lambda^{(d)}$ such that, for any lattice basis $w_1, \ldots, w_{d-1}$ of $\Lambda^{(d-1)}$, $w_1^{\sim}, \ldots, w_{d-1}^{\sim}, w$ is a lattice basis for $\Lambda^{(d)}$. If, moreover, the generator is a subgenerator of an MRG of order k and if $d > k$, then one can take $w = S^{d-k-1}(w_{\mathrm{ch}})$ where w_{ch} is given by (5).*

Proof. By (a), any $w \in \Lambda^{(d)}$ of minimal (positive) distance to the hyperplane $\mathbf{R}^{d-1} \times \{0\}$ will form, together with any basis of $\Lambda^{(d-1)} \times \{0\}$, a basis of $\Lambda^{(d)}$. In case of a subgenerator of an MRG, we note that, by Proposition 2, all corresponding lattices $\Lambda^{(d)}$ have the same volume for $d \geq k$. We further have, from Proposition 5, that $S^{d-k-1}(w_{\mathrm{ch}}) \in \Lambda^{(d)}$. Since the lattice generated by this vector and $\Lambda^{(d-1)} \times \{0\}$ has the same volume as $\Lambda^{(d-1)}$, and therefore as $\Lambda^{(d)}$, it must be equal to $\Lambda^{(d)}$. □

In the case of an arbitrary generator, an efficient algorithm for the determination of the vector w in the above proposition will be given in the last section.

Example 5. We consider the following two MRGs. The first is homogeneous, has modulus $m_1 = 2^{24}$ and characteristic polynomial $X^{97} + X^{64} - 1$. We denote by μ_1 its canonical unit. The second has modulus $m_2 = 2^{24} - 3$ (a prime), characteristic polynomial $X - 1$, and is inhomogeneous with increment $-7654321\mu_2$ where μ_2 denotes its canonical unit. Their product MRG has modulus $m = m_1 m_2$ and characteristic polynomial

$$X^{97} - 187649956511744\,X^{96} - 187649956511743\,X^{64} - 93824969867265.$$

It is thus of order 97. Let Σ be its state space. Then Σ^{r} is the state space of the corresponding combined generator. This combined generator closely approximates (the error is less than $3/m_1$) the generator proposed by Marsaglia, Zaman and Tsang [10], which is also known as RANMAR (see [4]). We introduce on Σ^{r} (also equal to Σ^{r}_0) the product ring structure of its components. The unit element is $\mu^{\mathrm{r}} = (\mu_1, \mu_2)$ and its ideals (each ideal in the product is the product of component ideals; see also Example 4) are then of the form $(n\mu^{\mathrm{r}})$ where the parameter n is a positive divisor of m. Table 1 gives spectral test results up to dimension $d = 100$, in the form of the reciprocal of the length of the shortest non-zero vector in $\Lambda^{(d)}$, for the product MRG (line $l = -1$), and for the homogeneous subgenerators contained in Σ^{r} and satisfying the condition of Proposition 1. The latter have, as state spaces, ideals of Σ^{r} with parameter $n = 2^l$, $l = 0, \ldots, 24$, and the results appear on the l-th line. The dimension is indicated on the top line.

TABLE 1. Successive hyperplane distances for RANMAR

l	$d \leq 97$	$d = 98$	$d = 99$	$d = 100$
-1	$1/(2^{48} - 3 \cdot 2^{24})$	$1/(\sqrt{2} \cdot 2^{24})$	$1/(\sqrt{2} \cdot 2^{24})$	$1/(\sqrt{2} \cdot 2^{24})$
0	$1/(\sqrt{2} \cdot 2^{24})$	$1/((2^{24} - 3)^2 + 18)^{1/2}$	$1/\sqrt{6}$	$1/\sqrt{6}$
1	$1/(\sqrt{2} \cdot 2^{23})$	$1/(2(2^{23} - 3)^2 + 9)^{1/2}$	$1/\sqrt{6}$	$1/\sqrt{6}$
2	$1/(\sqrt{2} \cdot 2^{22})$	$1/(\sqrt{2} \cdot 2^{22})$	$1/\sqrt{6}$	$1/\sqrt{6}$
$\vdots$	$1/(\sqrt{2} \cdot 2^{24-l})$	$1/(\sqrt{2} \cdot 2^{24-l})$	$1/\sqrt{6}$	$1/\sqrt{6}$
24	$1/\sqrt{2}$	$1/\sqrt{2}$	$1/\sqrt{2}$	$1/\sqrt{2}$

The lattices $\Lambda^{(d)}$ corresponding to Σ are described by Proposition 5. If $d \leq 97$, the length of the shortest non-zero vector of $\Lambda^{(d)}$ is obviously equal to m. For $d > 97$, we write $\mathbf{R}^d$ as a sum of orthogonal subspaces $\mathbf{R}^d = V_1 \oplus V_2$ where V_1 is generated by the set of e_i which are orthogonal to $w_{\mathrm{ch}}, Sw_{\mathrm{ch}}, \ldots, S^{d-98}w_{\mathrm{ch}}$ (w_{ch} is given by (5)). This splits the lattice $\Lambda^{(d)}$ and, since $\Lambda^{(d)} \cap V_1 = \mathbf{Z}^d \cap V_1$, we are reduced to examining the lattice $\Lambda^{(d)} \cap V_2$ with V_2 of dimension 4 (resp. 8, 12) for $d = 98$ (resp. 99, 100). For instance, if $d = 98$, we are led to the lattice in $\mathbf{R}^4$ generated by $-93824969867265e_1 - 187649956511743e_2 - 187649956511744e_3 + e_4$, me_2, me_3, and me_4. Thus, applying the spectral test to our product generator is easily performed by standard algorithms (such as in [2]), at least if the dimension is not much larger than 97. The results for this case are indicated in line $l = -1$ of the table.

For later use, we define $H^{(d)} \subset \mathbf{R}^d$ as the hyperplane $\{\sum_i x_i e_i \,|\, \sum_i x_i = 0\}$. Note that the distance of $\sum_i x_i e_i \in \mathbf{R}^d$ to $H^{(d)}$ is equal to $(1/\sqrt{d})|\sum_i x_i|$.

We now turn to the case of the combined generator (the subgenerator over $\Sigma^{\mathrm{r}} = (\mu^{\mathrm{r}})$, case $l = 0$). The lattice $\Lambda^{(d)}$ is the intersection of the lattices $\Lambda^{(d)}$ associated with the two components, and described by Proposition 5 and Example 3, respectively. If $d \leq 97$ it is thus equal to $\{m_1 \sum_i x_i e_i \,|\, x_i \in \mathbf{Z},\, \sum_i x_i \equiv 0 \pmod{m_2}\}$. Since any vector in this lattice of length less than m has at least two non-zero coordinates, the set of vectors of minimal length must be $\{m_1(e_i - e_j) \,|\, i \neq j\}$. If $d = 98$, we have in $\Lambda^{(d)}$, according to (a) and (b), the vectors $m_1(e_i - e_j)$ for all $i \neq j$. We also have the vector $m_2(-e_1 + e_{65} + e_{98})$ by applying (c) with $P_1(X) = X^{97} + X^{64} - 1$, $P_2(X) = m_2$, and using Proposition 5 and Example 3. From these we obtain that the following system of vectors $(1 \leq i \leq 98)$:

$$\begin{aligned} w_i &= m_2(-e_1 + e_{65} + e_{98}) - m_1(-e_1 + e_{65}) + m_1(e_i - e_{98}) \\ &= m_1 e_i + 3(e_1 - e_{65} - e_{98}) \end{aligned} \tag{8}$$

also belongs to $\Lambda^{(d)}$. These happen to form a lattice basis for $\Lambda^{(d)}$ since the equivalent system $m_2(-e_1 + e_{65} + e_{98})$, $m_1(e_i - e_{i+1})$, $i = 1, \ldots, 97$ has its determinant (namely $m_1^{97} m_2$) equal to the volume of $\Lambda^{(d)}$ (see Proposition 2). As they are (relatively) small perturbations of the vectors $m_1 e_i$, it is easy to show that a lattice vector of minimal length must be among them. In fact, any lattice vector $\sum_i c_i w_i$ satisfies $\|\sum_i c_i w_i\| \geq (m_1 - 18)\{\sum_i c_i^2\}^{1/2}$ and, if at least two of the integer coefficients c_i are not zero, this is larger than any of the $\|w_i\|$s. The least among these is computed to be $(m_2^2 + 18)^{1/2}$. If $d = 99$ or 100, one can again use (c) with $P_1(X) = X^{97} + X^{64} - 1$ and $P_2(X) = X - 1$ obtaining, in $\Lambda^{(d)}$, the vector $e_1 - e_2 - e_{65} + e_{66} - e_{98} + e_{99}$ (and also $e_2 - e_3 - e_{66} + e_{67} - e_{99} + e_{100}$ for $d = 100$) of length $\sqrt{6}$. These are vectors of minimal length in $\Lambda^{(d)}$. Indeed, assume for instance, that $d = 99$. A lattice basis for $\Lambda^{(d)}$ is then, by Proposition 8, $m_2(-e_1 + e_{65} + e_{98})$, $m_1(e_i - e_{i+1})$, $i = 1, \ldots, 97$, together with the vector $e_1 - e_2 - e_{65} + e_{66} - e_{98} + e_{99}$. All these vectors are contained in the hyperplane $H^{(99)}$, with the exception of $m_2(-e_1 + e_{65} + e_{98})$ whose distance to $H^{(99)}$, which is equal to $m_2/\sqrt{99}$, exceeds $\sqrt{6}$. It follows that a vector of length not exceeding $\sqrt{6}$ can be expressed as $x(e_1 - e_2 - e_{65} + e_{66} - e_{98} + e_{99}) + w$ with an integer $x \not\equiv 0 \pmod{m_1}$, and $w \in m_1 \mathbf{Z}^d$. Such a minimal length vector must therefore have at least 6 non-zero coordinates, so that its length should be at least $\sqrt{6}$.

Comparing values obtained thus far (see Table 1, lines $l = -1$ and $l = 0$), we remark that the product generator has, for $d = 99$ and 100, much smaller values (maximal hyperplane distances) than its subgenerator over the set of recurrent states. Thus, when studying the combined generator, one should beware of confusing it with the product generator since the former has a much coarser lattice structure.

The homogeneous subgenerators defined over $(2^l\mu^{\mathrm{r}})$, $0 < l \leq 24$, are (additively) isomorphic to the combined generator with the same components, with the difference that the first component now has modulus $m_1/2^l$. If $l = 24$, this combined generator is degenerate since it is reduced to its second component. Its associated lattice $\Lambda^{(d)}$ is described in Example 3, and has a shortest vector of length $\sqrt{2}$ in every dimension. So we will assume that $l < 24$. If $d < 98$ or if $d = 99$ or 100, the same arguments as for the case $l = 0$ show that the shortest vector in $\Lambda^{(d)}$ has length $(m_1/2^l)\sqrt{2}$ or $\sqrt{6}$ respectively. If $d = 98$, we must consider separately two cases. We first assume $l = 1, 2$ or 3. The argument is then similar to that used above in case $l = 0$. However, one should use as a lattice basis for $\Lambda^{(d)}$, instead of (8), the system $(1 \leq i \leq 98)$:

$$\begin{aligned} w_i &= m_2(-e_1 + e_{65} + e_{98}) - m_1(-e_1 + e_{65}) + \frac{m_1}{2^l}(e_i + \sum_{h=0}^{2^l-2} e_{98-h} - 2^l e_{98}) \\ &= \frac{m_1}{2^l}(e_i + \sum_{h=0}^{2^l-2} e_{98-h}) + 3(e_1 - e_{65} - e_{98}). \end{aligned}$$

We have $w_i = (m_1/2^l)w_i' + \epsilon$ with $w_i' = e_i + \sum_{h=0}^{2^l-2} e_{98-h}$, the second term $\epsilon = 3(e_1 - e_{65} - e_{98})$ being rather small compared with the first. Let $w = \sum_i c_i w_i$ with integral coefficients c_i, and put $w' = (m_1/2^l)\sum_i c_i w_i'$. Then $w' = (m_1/2^l)\sum_i c_i' e_i$ with $c_i' = c_i$ if $i < 100 - 2^l$, and $c_i' = c_i + \sum_j c_j$ otherwise. It follows that $\sum_i c_i' = 2^l \sum_i c_i$ and that

$$\|w - w'\| \leq 2^{-l}\, |\sum_i c_i'|\, \|\epsilon\| \leq \frac{60}{m_1}\|w'\|.$$

The determination of the length of the shortest non-zero vector w is thus reduced to the determination of all non-zero vectors $\sum c_i w_i'$, with integral c_i, of minimal length. This minimal length is equal to $\sqrt{2}$ and, if $l = 1$ (resp. $l = 2, 3$), the corresponding vectors have at most three (resp. two) non-zero coefficients c_i which are, moreover, equal to ± 1 (notice that, if $l = 1$ then the minimal length vectors $\sum c_i w_i' = \sum c_i' e_i$ must satisfy $c_i = c_i'$ for all $i < 98$, and when $l > 1$, $c_i = c_i'$ for all i since then $\sum_i c_i = 0$). Finally, if $l > 3$ then the vector $m_2(-e_1 + e_{65} + e_{98})$ has its distance to $H^{(98)}$ larger than $(m_1/2^l)\sqrt{2}$ so that a shortest non-zero vector of $\Lambda^{(d)}$ must be in $(m_1/2^l)\mathbf{Z}^d \cap H^{(98)}$ and is thus of length equal to $(m_1/2^l)\sqrt{2}$.

7. Lattice basis extension algorithms

Given a basis $w_1, \ldots, w_{d-1}$ for the lattice $\Lambda^{(d-1)}$ associated with an arbitrary generator (Σ, T, Φ), it is shown in Proposition 8 that there exists a vector $w \in \mathbf{R}^d$ such that $w_1, \ldots, w_{d-1}, w$ is a lattice basis for $\Lambda^{(d)}$. We describe, in this section, an (efficient) algorithm for the construction of this vector w. Let $M \subset (\mathbf{R}/\mathbf{Z})^d$ be the subgroup generated by all differences of elements of $\Phi^{(d)}(\Sigma)$. The algorithm assumes given any convenient generating system for M.

Example 6. Let (Σ, T, Φ) be an MRG of order k, canonical unit μ, and put $\tau = T_0(\mu)$. Consider the subgenerator of this MRG, defined over the T-orbit of $\sigma_0 \in \Sigma$, and its associated group M. By Proposition 2 and Example 2, M is the image under

$\Phi_0^{(d)}$ of the subgroup generated by the forward T_0-orbit of $\sigma'_0 = T_\Delta(\sigma_0)$. In terms of the canonical ring structure for the MRG, this subgroup is the ideal generated by σ'_0. We see therefore that M is generated by the image under $\Phi_0^{(d)}$ of the set $\sigma'_0, \ldots, \sigma'_0\tau^{k-1}$. Similarly, this time using Example 1, the group M corresponding to the subgenerator defined over Σ^{r} is the image under $\Phi_0^{(d)}$ of the ideal generated by a sufficiently high power τ^l so that $(\tau^{l+1}) = (\tau^l)$. This is certainly satisfied if $2^l > m^k$, m being the modulus of the MRG. In this case, the group M is generated by the image under $\Phi_0^{(d)}$ of the set $\tau^l, \ldots, \tau^{l+k-1}$.

Let m be an integer such that $mM = 0$, so that M is an A-module where $A = \mathbf{Z}/m\mathbf{Z}$. For $v \in M$ define $\phi_i(v) \in A$ as the i-th coordinate of v (defined modulo 1) multiplied by m. This gives a system of A-linear forms $\phi_1, \ldots, \phi_d \in M^\star$ which is *complete* in the sense that, if $\phi_i(v) = 0$ for all i, then $v = 0$.

The main step of the algorithm is to transform the given generating system into a system of vectors $v_1, \ldots, v_d \in M$ with the following properties.

i) $\phi_j(v_i) = 0$ if $i > j$;
ii) $\phi_j(v_j) = 0$ implies $v_j = 0$;
iii) $v \in M$ and $\phi_l(v) = 0$ for all $l < j$ imply $v \in \sum_{l \geq j} Av_l$;
iv) $\phi_j(v_j)$ has a representative which divides m.

For this, we recursively construct d other systems (which may not generate M) as follows. Let $u_1, \ldots, u_l$ be the j-th system (the first system is the given generating system). If $\phi_j(u_i) = 0$ for all i, we put $v_j = 0$, and take the $(j+1)$-th system to be identical to the j-th. Otherwise, let $\mathfrak{a}$ be the (non-zero) ideal of A generated by the elements $\phi_j(u_i), i = 1, \ldots, l$, and construct $u'_1, \ldots, u'_{l+1}$, generating the same submodule as the j-th system, such that $\phi_j(u'_i) = 0$ for all $i < l+1$, and such that $\phi(u'_{l+1})$ generates the ideal $\mathfrak{a}$. This is done by using the Euclidean algorithm to determine $a_1, \ldots, a_l$ and $b_1, \ldots, b_l \in A$ such that $a = a_1\phi(u_1) + \cdots + a_l\phi(u_l)$ generates $\mathfrak{a}$, and $\phi(u_i) = b_i a$ for all $i < l+1$; then take $u'_{l+1} = a_1u_1 + \cdots + a_lu_l$ and $u'_i = u_i - b_iu'_{l+1}$ for $i < l+1$. Finally, put $v_j = u'_{l+1}$, and take the $j+1$-th system to be $v'_1, \ldots, v'_l, a_0v'_{l+1}$ where a_0 is a generator for the ideal $\{y \in A | y\phi_j(u'_{l+1}) = 0\}$.

We now verify the first 3 properties for the system $v_1, \ldots, v_d$. One can easily verify, by induction on j, that if u belongs to the j-th system as above, then $\phi_l(u) = 0$ for $l < j$ and, since v_j is chosen in the submodule generated by the j-th system, we also have $\phi_l(v_j) = 0$. This proves the first property. The second is immediate from the construction. To prove the third, notice that $v_j, \ldots, v_d$ generate the same submodule as the j-th system. In particular, $v_1, \ldots, v_d$ generate M. Any $v \in M$ can therefore be written as $v = \sum_l a_lv_l$. Choose, among such expressions, that for which the index of the first non-zero coefficient is maximal. If this index is $j_0 < j$, and if $\phi_l(v) = 0$ for $l < j$, we have $a_{j_0}\phi_{j_0}(v_{j_0}) = 0$ and, by construction, $a_{j_0}v_{j_0}$ belongs to the submodule generated by the (j_0+1)-th system, contradicting the maximality property j_0. Finally, one can achieve property iv) by multiplying v_i by a suitable invertible element of A. This does not affect the validity of i)–iii).

Proposition 9. *If $v_1, \ldots, v_d \in M$ satisfy the above properties* i)–iv)*, then any set of vectors $\bar{v}_1, \ldots, \bar{v}_d \in \mathbf{R}^d$ satisfying*

i) $\mathrm{can}(\bar{v}_i) = v_i$ *and the first $i-1$ coordinates of $\bar{v}_i$ are 0;*
ii) *if $v_i \neq 0$, then the i-th coordinate of $\bar{v}_i$ is the inverse of an integer;*

iii) *if* $v_i = 0$, *then* $\bar{v}_i = e_i$;

is a lattice basis for the inverse image of M *(and therefore for* Λ_d*) by the mapping* (1).

Proof. It is sufficient to show that $\mathbf{Z}^d$ is contained in the subgroup generated by the $\bar{v}_i$'s. We show recursively that e_i is in the subgroup generated by $\bar{v}_i, \ldots, \bar{v}_d$. This is clear for $i = d$ or if $v_i = 0$. Assume the fact true for $i+1$, and $v_i \neq 0$. By ii) there is an integer c_i such that the i-th coordinate of $\bar{v} = e_i - c\bar{v}_i$ is zero. If $v = \mathrm{can}(\bar{v})$, then $\phi_j(v) = 0$ if $j \leq i$ so that $v \in \sum_{l>j} Av_l$ (see above the proposition, item iii). This implies that $\bar{v}$ belongs to the subgroup generated by $\bar{v}_{i+1}, \ldots, \bar{v}_d$ and $\mathbf{Z}^d$. From our assumption for $i+1$, $\bar{v}$ actually belongs to the subgroup generated by $\bar{v}_{i+1}, \ldots, \bar{v}_d$ since all these vectors (including $\bar{v}$) have their first i coordinates equal to zero. We conclude that $e_i = \bar{v} + c\bar{v}_i$ belongs to the subgroup generated by $\bar{v}_i, \ldots, \bar{v}_d$. $\square$

Any choice of a basis $\bar{v}_1, \ldots, \bar{v}_d$ for Λ_d satisfying the conditions in the above proposition can then be used to determine a vector w by the conditions $\bar{v}_i \cdot w = 0$ for $i < d$ and $\bar{v}_d \cdot w = 1$. This is the sought for vector since it clearly belongs to $\Lambda^{(d)}$, and it generates, with $\Lambda^{(d-1)} \times \{0\}$, a lattice of the same volume as $\Lambda^{(d)}$.

Acknowledgments

We wish to thank the referee, who pointed out missing assumptions in an earlier version of the manuscript and gave several suggestions which have improved the paper.

References

1. R. Couture and P. L'Ecuyer, *On the Lattice Structure of certain Linear Congruential Sequences related to AWC/SWB Generators*, Math. Comp. **62**, (1994), 798–808.
2. U. Fincke and M. Pohst, *Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis*, Math. Comp. **44** (1985) 463–471.
3. A. Grube, *Mehrfach rekursiv-erzeugte Pseudo-Zufallszahlen*, Z. Angew. Math. Mech. **53**, (1973), T223–T225.
4. F. James, *A review of pseudorandom number generators*, Comp. Phys. Comm. 60 (1990) 329–344.
5. D. E. Knuth, *The Art of Computer Programming : Seminumerical Algorithms*, vol. 2, second edition. Addison-Wesley, 1981.
6. P. L'Ecuyer, *Combined Multiple Recursive Generators*, Submitted.
7. P. L'Ecuyer, F. Blouin, and R. Couture, *A Search for Good Multiple Recursive Random Number Generators*, ACM Trans. Modeling and Computer Simulation, **3**, 2 (1993) 87–98.
8. P. L'Ecuyer and R. Couture, *An Implementation of the Lattice and Spectral Tests for Linear Congruential and Multiple Recursive Generators*, Submitted.
9. P. L'Ecuyer and S. Tezuka, *Structural Properties for Two Classes of Combined Random Number Generators*, Math. Comp. **57**, 196 (1991) 735–746.
10. G. Marsaglia, A. Zaman, W.-W. Tsang, *Toward a Universal Random Number Generator*, Stat. Prob. Lett. 9 (1990) 35–39.
11. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 63, SIAM, Philadelphia (1992).
12. B. A. Wichmann and I. D. Hill, *An Efficient and Portable Pseudo-random Number Generator.* Appl. Statist. **31** (1982) 188–190.

Département d'Informatique, Université Laval, Ste-Foy, G1K 7P4, Canada
E-mail address: couture@iad.ift.ulaval.ca

Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal, H3C 3J7, Canada
E-mail address: lecuyer@iro.umontreal.ca