1. Introduction

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

$$T : \Sigma \rightarrow \Sigma$$

determining the evolution of the system, and an output mapping

$$\Phi : \Sigma \rightarrow \mathbb{Q}/\mathbb{Z}.$$  

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

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

of pseudorandom numbers. One can associate with such a system $(\Sigma, T, \Phi)$, and each positive integer $d$, a lattice $\Lambda_d$ in $\mathbb{R}^d$ as follows. First, we define the mapping

$$\Phi^{(d)} : \Sigma \rightarrow (\mathbb{R}/\mathbb{Z})^d$$

by

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

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

$$(1) \quad \text{can} : \mathbb{R}^d \rightarrow (\mathbb{R}/\mathbb{Z})^d,$$

of the subgroup of $(\mathbb{R}/\mathbb{Z})^d$ generated by all differences between any two elements of $\Phi^{(d)}(\Sigma)$. The structure of the lattice $\Lambda_d$ is indicative of the distribution of the set of all (overlapping) $d$-tuples of successive values of the generator. Determining the length of the shortest vector of the dual lattice $\Lambda^{(d)}$ to $\Lambda_d$, 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 \(\Sigma\) 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 \(\Lambda_d\). These
will be contained, strictly in general, in the corresponding lattices defined by \(\Sigma\).

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 \(\bigcap_i T^i(\Sigma)\), which is especially interesting, since it is precisely the
set \(\Sigma'\) of recurrent states. If this set quickly attracts into it an arbitrary state, then
the lattices associated with \(\Sigma'\) are more relevant to the behavior of the generator
than those associated with \(\Sigma\).

We will discuss this question for the class, defined in \(\S 3\), 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 \(\S 2\) how their study can be reduced to that of corresponding homogeneous
generators. Combination, as defined in \(\S 4\), is a standard construction in the design
of random number generators [6, 12]. Although the combination of MRGs is, in
general, not an 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 \(\S 7\). We illustrate, in \(\S 6\), 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 ge-
erators \((\Sigma_1, T_1, \Phi_1)\) and \((\Sigma_2, T_2, \Phi_2)\) 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 \(\Lambda_d\) 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 parallelepiped generated by one of its bases. For
a vector \(v \in \mathbb{R}^d\) we denote by \(v^\sim\) the vector in \(\mathbb{R}^{d+1}\) obtained from \(v\) by adding a
zero coordinate. We will denote by \(e_i, i = 1, \ldots, d\), the canonical basis for \(\mathbb{R}^d\) —so
that \(e_i^\sim = e_i \uparrow\) — and by \(S\) the (linear) right-shift on \(\mathbb{R}^d\) 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 \((\Sigma, T, \Phi)\) is additive if its state space \(\Sigma\) 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 \( \Phi \), is a group homomorphism. The generator \((\Sigma, T_0, \Phi)\) 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 \( \Sigma_0' \) 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 \((\Sigma, T_0, \Phi)\) given by a subgroup of \( \Sigma \)). 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 characterized algebraically in \( \S 5 \).

**Example 1.** The set \( \Sigma' \) of recurrent states of an additive generator \((\Sigma, T, \Phi)\) is obviously \( T \)-invariant, and the corresponding homogeneous subgenerator is defined by the subgroup \( \Sigma_0' \) of recurrent states with respect to \( T_0 \). Indeed, if \( \sigma_1, \sigma_2 \in \Sigma' \) 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 \( \sigma_1 - \sigma_2 \in \Sigma_0' \). Conversely, if \( \sigma \in \Sigma_0' \) and \( \sigma_2 \in \Sigma' \), 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 \( \sigma \) and \( \sigma_2 \) (relative to \( T_0 \) and \( T \), respectively). We thus obtain \( \sigma + \sigma_2 \in \Sigma_0' \).

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

\[
T_\Delta(\Sigma') \subset \Sigma_0'.
\]

**Lemma 1.** The mapping \( T_\Delta \) 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 \( T_\Delta \circ T(\sigma) = T^2(\sigma) - T(\sigma) = T_0 \circ T(\sigma) - T_0(\sigma) = T_0 \circ T_\Delta(\sigma). \)

**Example 2.** If \( \Sigma' \) is the forward \( T \)-orbit of \( \sigma_0 \) then, by Lemma 1, \( T_\Delta(\Sigma') \) is the forward \( T_0 \)-orbit of \( T_\Delta(\sigma_0) \). Therefore, in this case, \( \Sigma_0' \) 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 \( \Sigma_0' \) for some \( T \)-invariant subset \( \Sigma' \). We have

**Proposition 1.** A \( T_0 \)-invariant subgroup of \( \Sigma \) is of the form \( \Sigma_0' \) for some \( T \)-invariant subset \( \Sigma' \) of \( \Sigma \) if and only if it has a nonvoid intersection with \( T_\Delta(\Sigma) \).

**Proof.** By (2), the condition is clearly necessary. Conversely, assume \( \Sigma_1 \) is a \( T_0 \)-invariant subgroup and that \( T_\Delta(\sigma') \in \Sigma_1 \). Put \( \Sigma' = \sigma' + \Sigma_1 \). Then \( \Sigma' \) 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 \( \Sigma_0' = \Sigma_1 \).

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 \( \Phi_0^{(d)} : \Sigma \to (\mathbb{R}/\mathbb{Z})^d \) 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 \( \Lambda_d \) 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.
It follows that \( R \) such that \( 0. \) The Euclidean algorithm provides us with polynomials \( Q \) as \( \sigma \)

**Proposition 3.** For an MRG \( T \) generic \( \Sigma \) is an \( f \)-group and the output mapping \( \Phi \) is \( \text{generic} \) in the sense that its kernel contains no nonzero forward \( T_0 \)-orbit.

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

\[
\Phi(T_0^{-1}(\mu)) = (1/m) \delta_k, \quad i = 1, \ldots, k.
\]

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

**Proposition 4.** For an MRG \( (\Sigma, T, \Phi) \) with modulus \( m \) and characteristic polynomial \( P_{\text{ch}}(X) \), the following conditions on \( P(X) = \mathbb{Z}/m\mathbb{Z}[X] \), are equivalent:

(i) \( P(T_0)(\mu) = 0 \),

(ii) \( P(T_0) = 0 \),

(iii) \( P_{\text{ch}}(X) \) divides \( P(X) \).

In particular, \( P_{\text{ch}}(X) \) 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 \( P_1(X) \in \mathbb{Z}/m\mathbb{Z}[X] \), and \( P(T_0)(\sigma) = P_1(T_0)P(T_0)(\mu) = 0 \). The Euclidean algorithm provides us with polynomials \( Q(X), R(X) \in \mathbb{Z}/m\mathbb{Z}[X] \) 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 $(\Sigma_1, T_1, \Phi_1)$ and $(\Sigma_2, T_2, \Phi_2)$, with respective canonical units $\mu_1$ and $\mu_2$. Assume there is an additive isomorphism $f : \Sigma_1 \to \Sigma_2$ between them. Clearly $\Sigma_1$ and $\Sigma_2$ 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

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

The first statement in the proposition follows. Since $\Phi_2 \circ f = \Phi_1$, we obtain, using (4), $\Phi_{2,0} \circ f = \Phi_{1,0}$, $k$ being the order. It follows that $f(\mu_1) = \mu_2$ and, again using (4), that $f(T_{1,0}(\mu_1)) = T_{2,0}(\mu_2)$ 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 $P(X) \in \mathbb{Z}/m\mathbb{Z}[X]$ 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 $(\Sigma, T, \Phi)$ to a monic polynomial $X^k - a_1X^{k-1} - \cdots - a_k \in \mathbb{Z}[X]$, and put

$$b = \Phi(T^k(0) - a_1T^{k-1}(0) - \cdots - a_kT^0(0)),$$

the output sequence $u_i = \Phi(T^i(\sigma_0)) \in \mathbb{Q}/\mathbb{Z}$, $i = 0, 1, \ldots$, 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 $(1/m)\mathbb{Z}/\mathbb{Z}$ 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 $\Lambda_d$ and $\Lambda^{(d)}$ associated with an MRG are determined by its modulus and characteristic polynomial. In particular, if we put, for $d > k$,

$$w_{\text{ch}} = -a_k \epsilon_1 - \cdots - a_1 \epsilon_k + \epsilon_{k+1},$$

we have the following.

**Proposition 5.** If $d \leq k$, then $\Lambda^{(d)} = m\mathbb{Z}^d$. If $d > k$, then $\Lambda^{(d)}$ admits the lattice basis $m\epsilon_1, \ldots, m\epsilon_k, w_{\text{ch}}, Sw_{\text{ch}}, \ldots, S^{d-k-1}w_{\text{ch}}$.

Proof. Since $\Phi$ is generic, $\Phi^{(d)}_{\sigma_0}(\Sigma)$ is the subgroup $((1/m)\mathbb{Z}/\mathbb{Z})^d$ 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 $\Lambda^{(d)}$. \qed

4. Products and extensions of MRGs

From a given finite family of generators $(\Sigma_i, T_i, \Phi_i)$ 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 $\Lambda_d$ (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 $P_{ch}(X)$ is determined by the conditions $P_{ch}(X) \equiv P_{ch,i}(X) \pmod{m_i}$, where $P_{ch,i}(X)$ 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 $P_{ch}(X)$ satisfying $P_{ch}(X) \equiv X^{k_i}P_{ch,i}(X) \pmod{m_i}$. 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 $(\Sigma, \bar{T}, \Phi)$ 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 $\Sigma$. When both generators are additive, we will say that the extension is additive if $\Sigma$ is a subgroup of $\bar{\Sigma}$. The increments $T(0)$ and $\bar{T}(0)$ are then equal and contained in $\Sigma$. 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 $\Sigma$ eventually ends up in $\Sigma$.

**Lemma 2.** Assume that $(\Sigma, \bar{T}, \Phi)$ is a nil-extension of $(\Sigma, T, \Phi)$. Let $\bar{k}$, $\bar{P}_{ch}(X)$, $\bar{\mu}$, and $\bar{k}$, $P_{ch}(X)$, $\mu$ be their respective order, characteristic polynomial, and canonical unit. If the integer $i$ is sufficiently large, so that $T^i_0(\Sigma) \subset \Sigma$, then $i \geq \bar{k} - k$. If $T^\bar{k} - k_0(\Sigma) \subset \Sigma$, then $\bar{P}_{ch}(X) = X^{k}P_{ch}(X)$, and $T^\bar{k} - k(\mu) = \mu$.

**Proof.** Assume $T^i_0(\Sigma) \subset \Sigma$ with $i < \bar{k} - k$. Then $T^i_0(\mu) \in \Sigma$ is not 0, but $\Phi(T^i_0 + j(\mu)) = 0$ for $0 \leq j < k$, contradicting the genericity of $\Phi$.

If $T^{\bar{k} - k}_0(\Sigma) \subset \Sigma$, then, by Proposition 3, we have $\bar{P}_{ch}(X) | X^{\bar{k} - k}P_{ch}(X)$. 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 $T^{\bar{k} - k}_0(\mu) \in \Sigma$ satisfies the conditions (3) defining $\mu$.

If a nil-extension satisfies (with the above notations) $T^{\bar{k} - k}_0(\Sigma) \subset \Sigma$, 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 $(\Sigma, T, \Phi)$ be the given generator, $m$ its modulus and $\mu$ its canonical unit. Embed $\Sigma$ 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 $\Sigma$ (so that $\bar{\Sigma} = \Sigma \oplus \Sigma'$), and choose a $\mathbb{Z}/m\mathbb{Z}$-basis, $\mu_1, \ldots, \mu_{\bar{k} - k}$ for $\Sigma'$. Define $\bar{T} : \Sigma \to \bar{\Sigma}$ so that its restriction to $\Sigma$ is equal to $T$, and such that $\bar{T}_0$ is a 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 $\Phi$ to be equal to $\Phi$ on $\Sigma$, and 0 on $\Sigma'$. Then $(\Sigma, \bar{T}, \Phi)$ is the required extension. Two nil-extensions of the same order are (additively) isomorphic by Proposition 4 and the preceding lemma.

We can now define the product MRG of a finite family of MRGs $(\Sigma_i, T_i, \Phi_i)$ 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 $\prod_i \Sigma_i$.
5. A ring structure for MRGs

One can introduce a ring structure in several ways in the state space of an MRG $(\Sigma, T, \Phi)$ so that the action of $T_0$ is the same as multiplication by some fixed element of $\Sigma$. 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 $(\Sigma, T, \Phi)$ such that

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

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

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

$$Z/mZ[X]/(P_{ch}(X)) \simeq \Sigma.$$  

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

We notice that, in terms of the canonical ring structure, a $T_0$-invariant subgroup is the same as an ideal of $\Sigma$, while the subgroup generated by the forward $T_0$-orbit of some element in $\Sigma$ 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 $\Sigma$.

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

$$\Sigma \to \bar{\Sigma} = \Sigma/p.$$  

Let $\bar{\tau}$ be the image of $\tau$ in $\bar{\Sigma}$. Let $\bar{P}_{ch}(X) \in F_p[X]$ be the polynomial obtained from $P_{ch}(X)$ by reducing its coefficients modulo $p$, and $\bar{P}_{ch}(X) = \prod_j \bar{P}_j^{e_j}(X)$ be its factorization into irreducible polynomials. Put $\bar{p}_j = (\bar{P}_j(\bar{\tau}))$, and let $p_j$ be its inverse image by (7) in $\Sigma$. The ideals $p_j$ are precisely the prime ideals (they are all, in fact, maximal) of $\Sigma$. More generally, any ideal of $\Sigma$ containing $p$ is the inverse image by (7) of an ideal of $\bar{\Sigma}$ of the form $\prod_j \bar{p}_j^{e_j}$, $0 \leq e_j \leq e_j$. The set of ideals of $\Sigma$ exhibited so far is still not sufficient to account for all ideals of $\Sigma$. For instance, if $m = 4$ and $\tau$ has minimal polynomial $P_0(X) = X^2$, then $\tau$ does not contain and is not contained in $p = (2)$, nor is it a product of ideals containing $p$. A simple situation however arises if $P_0(X) \in F_p[X]$ is irreducible. The ideals $p^{e_j}$, $e_j = 1, \ldots, e - 1$, are then the only proper ideals of $\Sigma$. Indeed, since $p$ is then the only maximal ideal, any element not contained in it is invertible. Let $a$ be any ideal of $\Sigma$, and $p^n$ the highest power of $p$ containing $a$. Then $a$ contains an element of the form $p^n\alpha$ with $\alpha \notin p$. Since $\alpha$ is then invertible, we obtain $a = p^n$.

6. Short vector search strategies

The search for short vectors in the dual lattices $\Lambda^{(d)}$ to $\Lambda_d$ is often facilitated by the following facts, valid for arbitrary (combined) generators:
It is thus of order 97. Let $\Sigma$ be its state space. Then $\Sigma^1$ 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 $\Sigma^*$ (also
equal to $\Sigma^r_0$) the product ring structure of its components. The unit element is $\mu^r = (\mu_1, \mu_2)$, and its ideals (each ideal in the product is the product of component ideals; see also Example 4) are then of the form $(n\mu^r)$, 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 $\Sigma^r$ and satisfying the condition of Proposition 1. The latter have, as state spaces, ideals of $\Sigma^r$ with parameter $n = 2^i$, $l = 0, \ldots, 24$, and the results appear on the $l$th line. The dimension is indicated on the top line.

**Table 1. Successive hyperplane distances for RANMAR**

<table>
<thead>
<tr>
<th>$l$</th>
<th>$d \leq 97$</th>
<th>$d = 98$</th>
<th>$d = 99$</th>
<th>$d = 100$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$1/(2^{48} - 3 \cdot 2^{24})$</td>
<td>$1/(\sqrt{2} \cdot 2^{24})$</td>
<td>$1/(\sqrt{2} \cdot 2^{24})$</td>
<td>$1/(\sqrt{2} \cdot 2^{24})$</td>
</tr>
<tr>
<td>1</td>
<td>$1/(\sqrt{2} \cdot 2^{23})$</td>
<td>$1/(2^{23} - 9 \cdot 2^{15} + 1)\sqrt{2}$</td>
<td>$1/\sqrt{6}$</td>
<td>$1/\sqrt{6}$</td>
</tr>
<tr>
<td>2</td>
<td>$1/(\sqrt{2} \cdot 2^{22})$</td>
<td>$1/(\sqrt{2} \cdot 2^{22})$</td>
<td>$1/\sqrt{6}$</td>
<td>$1/\sqrt{6}$</td>
</tr>
<tr>
<td>24</td>
<td>$1/\sqrt{2}$</td>
<td>$1/\sqrt{2}$</td>
<td>$1/\sqrt{2}$</td>
<td>$1/\sqrt{2}$</td>
</tr>
</tbody>
</table>

The lattices $\Lambda^{(d)}$ corresponding to $\Sigma$ are described by Proposition 5. If $d \leq 97$, the length of the shortest nonzero vector of $\Lambda^{(d)}$ is obviously equal to $m$. For $d > 97$, we write $\mathbb{R}^d$ as a sum of orthogonal subspaces $\mathbb{R}^d = V_1 \oplus V_2$, where $V_1$ is generated by the set of $e_i$ which are orthogonal to $w_{\text{ch}}, w_{\text{ch}^2}, \ldots, w_{\text{ch}^{d-98}}$ (where $w_{\text{ch}}$ is given by (5)). This splits the lattice $\Lambda^{(d)}$ into $\Lambda^{(d)} \cap V_1 = \mathbb{Z}^d \cap V_1$, 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 $\mathbb{R}^4$ 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 $H^{(d)} \subset \mathbb{R}^d$ as the hyperplane $\{\sum_i x_i e_i | \sum_i x_i = 0\}$. Note that the distance of $\sum_i x_i e_i \in \mathbb{R}^d$ 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 $\Sigma^r = (\mu^r)$, 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 $\{m_1 \sum_i x_i e_i | x_i \in \mathbb{Z}, \sum_i x_i \equiv 0 \pmod{m_2}\}$. Since any vector in this lattice of length less than $m$ has at least two nonzero 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 $\leq i \leq 98$):

$$
\begin{align*}
w_i &= m_2(-e_1 + e_65 + e_{98}) - m_1(e_i - e_65) + m_1(e_i - e_{98}) \\
&= m_1 e_i + 3(e_i - e_65 - e_{98})
\end{align*}
$$
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 $m_2^3 m_2$) 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 $\|\sum_i c_i w_i\| \geq (m_1 - 18)(\sum c_i^2)^{1/2}$ and, if at least two of the integer coefficients $c_i$ are not zero, this is larger than any of the $\|w_i\|$. 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 $x \neq 0$ (mod $m_1$), and $w \in m_1\mathbb{Z}^d$. Such a minimal length vector must therefore have at least six nonzero 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 $(2^l \mu')$, $0 < l \leq 24$, 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 $(m_1/2^l)^{1/2} \sqrt{2}$ 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 ($1 \leq i \leq 98$):

\[ w_i = m_2(-e_1 + e_{65} + e_{98}) - m_1(-e_1 + e_{65}) + \frac{m_1}{2^l}(e_i + \sum_{h=0}^{2^l-2} e_{98-h} - 2^l e_{98}) \]

\[ = \frac{m_1}{2^l}(e_i + \sum_{h=0}^{2^l-2} e_{98-h}) + 3(e_1 - e_{65} - e_{98}). \]

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
\[ \sum_i c_i' = 2^i \sum_i c_i \text{ and that} \]
\[ \|w - w'\| \leq 2^{-i} \left| \sum_i c_i' \right| \|e\| \leq \frac{60}{m_1} \|w'\|. \]

The determination of the length of the shortest nonzero vector \( w \) is thus reduced to the determination of all nonzero 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) nonzero coefficients \( c_i \) which are, moreover, equal to \( \pm 1 \) (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 nonzero vector of \( \Lambda^{(d)} \) must be in \( (m_1/2^l)\mathbb{Z}^d \cap H^{(98)} \) 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 \((\Sigma, T, \Phi)\), it is shown in Proposition 8 that there exists a vector \( w \in \mathbb{R}^d \) 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 \( M \subset (\mathbb{R}/\mathbb{Z})^d \) 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 \((\Sigma, T, \Phi)\) be an MRG of order \( k \), canonical unit \( \mu \), 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 \( \Phi^{(d)}_0 \) 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 \( \sigma'_0 \). We see therefore that \( M \) is generated by the image under \( \Phi^{(d)}_0 \) 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 \( \Sigma^* \) is the image under \( \Phi^{(d)}_0 \) of the ideal generated by a sufficiently high power \( \tau^i \) so that \( \tau^{i+1} = (\tau^i) \). This is certainly satisfied if \( 2^i > m^k \), \( m \) being the modulus of the MRG. In this case, the group \( M \) is generated by the image under \( \Phi^{(d)}_0 \) of the set \( \tau^i, \ldots, \tau^i+k-1 \).

Let \( m \) be an integer such that \( mM = 0 \), so that \( M \) is an \( A \)-module where \( A = \mathbb{Z}/m\mathbb{Z} \). 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 \( \phi_1, \ldots, \phi_d \in M^* \) 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 \( \phi_i(v) = 0 \) for all \( l < j \) imply \( v \in \sum_{\ell \geq j} A v_l \),
(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 \((j + 1)\)st system to be identical to the \( j \)th. Otherwise, let \( a \) be the (nonzero) 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 $a$. 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 $a$, and $\phi(u'_i) = b_ia$ 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 $(j + 1)$st system to be $v'_1, \ldots, v'_j, a_0v'_j$, where $a_0$ is a generator for the ideal $\{y \in A | y\phi_j(u'_{l+1}) = 0\}$.

We now verify the first three 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 $\phi_j(u) = 0$ for $l < j$ and, since $v_j$ is chosen in the submodule generated by the $j$th system, we also have $\phi_j(v_j) = 0$. 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 $v = \sum_i a_i v_i$. Choose, among such expressions, that for which the index of the first nonzero coefficient is maximal. If this index is $j_0 < j$, and if $\phi_j(v) = 0$ for $l < j$, we have $a_{j_0}\phi_j(v_{j_0}) = 0$ and, by construction, $a_{j_0}v_{j_0}$ belongs to the submodule generated by the $(j_0 + 1)$st 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 $\vec{v}_1, \ldots, \vec{v}_d \in \mathbb{R}^d$ satisfying

(i) $\text{can}(\vec{v}_i) = v_i$ and the first $i - 1$ coordinates of $\vec{v}_i$ are 0,

(ii) if $v_i \neq 0$, then the $i$th coordinate of $\vec{v}_i$ is the inverse of an integer,

(iii) if $v_i = 0$, then $\vec{v}_i = e_i$,

is a lattice basis for the inverse image of $M$ (and therefore for $\Lambda_d$) by the mapping (1).

**Proof.** It is sufficient to show that $\mathbb{Z}^d$ is contained in the subgroup generated by the $\vec{v}_i$’s. We show recursively that $e_i$ is in the subgroup generated by $\vec{v}_1, \ldots, \vec{v}_d$. 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 $\vec{v} = e_i - c\vec{v}$ is zero. If $v = \text{can}(\vec{v})$, then $\phi_j(v) = 0$ if $j < i$ so that $v \in \sum_{l < j} A\vec{v}_l$ (see the proposition above, item (iii)). This implies that $\vec{v}$ belongs to the subgroup generated by $\vec{v}_{i+1}, \ldots, \vec{v}_d$ and $\mathbb{Z}^d$. From our assumption for $i + 1$, $\vec{v}$ actually belongs to the subgroup generated by $\vec{v}_{i+1}, \ldots, \vec{v}_d$ since all these vectors (including $\vec{v}$) have their first $i$ coordinates equal to zero. We conclude that $e_i = \vec{v} + c\vec{v}$ belongs to the subgroup generated by $\vec{v}_1, \ldots, \vec{v}_d$.

Any choice of a basis $\vec{v}_1, \ldots, \vec{v}_d$ for $\Lambda_d$ satisfying the conditions in the above proposition can then be used to determine a vector $w$ by the conditions $\vec{v}_i \cdot w = 0$ for $i < d$ and $\vec{v}_d \cdot w = 1$. 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 $\Lambda(d)$.

**Acknowledgment**

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


DÉPARTEMENT D’INFORMATIQUE ET DE RECHERCHE OPÉRATIONNELLE, UNIVERSITÉ DE MONTRÉAL, C.P. 6128, SUCC. CENTRE-VILLE, MONTRÉAL, H3C 3J7, CANADA
E-mail address: couture@iro.umontreal.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