MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 202
APRIL 1993, PAGES 749-761

ON THE DISTRIBUTION OF k-DIMENSIONAL VECTORS FOR SIMPLE AND COMBINED TAUSWORTHE SEQUENCES

RAYMOND COUTURE, PIERRE L'ECUYER, AND SHU TEZUKA

ABSTRACT. The lattice structure of conventional linear congruential random number generators (LCGs), over integers, is well known. In this paper, we study LCGs in the field of formal Laurent series, with coefficients in the Galois field $\mathbb{F}_2$. The state of the generator (a Laurent series) evolves according to a linear recursion and can be mapped to a number between 0 and 1, producing what we call a LS2 sequence. In particular, the sequences produced by simple or combined Tausworthe generators are special cases of LS2 sequences. By analyzing the lattice structure of the LCG, we obtain a precise description of how all the k-dimensional vectors formed by successive values in the LS2 sequence are distributed in the unit hypercube. More specifically, for any partition of the k-dimensional hypercube into 2^{kl} identical subcubes, we can quickly compute a table giving the exact number of subcubes that contain exactly n points, for each integer n. We give numerical examples and discuss the practical implications of our results.

1. INTRODUCTION

Following Tezuka [12, 13], we consider the analogue of a multiplicative linear congruential generator in the field K of formal Laurent expansions (at infinity) with coefficients in the Galois field $\mathbb{F}_2$:

$$x = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \cdots , \tag{1}$$

where n is any integer. This generator is conveniently defined with the help of the operators

$$\operatorname{frac}(x) = \alpha_{-1} z^{-1} + \alpha_{-2} z^{-2} + \cdots ,$$
$$\operatorname{trunc}_l(x) = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \cdots + \alpha_{-l} z^{-l}$$

for $x \in K$ defined as in (1) and $l \in \mathbb{Z}$. Let a (the *multiplier*) and m (the *modulus*) be nonzero elements in K. For $l > 0$, we consider the pseudorandom

Received by the editor October 28, 1991.

1991 *Mathematics Subject Classification.* Primary 65C10.

This work has been supported by NSERC-Canada grant # OGP0110050, FCAR-Québec grant # EQ2831, and the Ministry of External Affairs and External Commerce of Canada, to the second author.

sequence

$$u_i = \mathrm{trunc}_l(\mathrm{frac}(a^i/m)), \qquad i = 0, 1, 2, \ldots. \tag{2}$$

One can identify any element x expressed as in (1) with the real number $\alpha_n 2^n + \alpha_{n-1}2^{n-1} + \cdots$, where each $\alpha_i \in \mathbb{F}_2$ is identified with its representative integer 0 or 1. The sequence (2) in K is then identified with a pseudorandom sequence in the interval $[0, 1)$, which we call a LS2 (Laurent Series over $\mathbb{F}_2$) sequence. As pointed out by Tezuka [12, 13], the usual Tausworthe sequences, as well as their combinations by means of addition modulo two, are instances of this scheme. Tezuka has also shown the influence of the last and first successive minima of certain lattices in K^k associated with combined generators, and with their components, on their k-distribution properties.

The aim of this paper is to show that a more complete description of the k-distribution involves all successive minima for the corresponding lattices. For any partition of the k-dimensional hypercube into 2^{kl} identical subcubes, we show how to quickly compute a table giving the number of subcubes that contain exactly n points, for each integer n.

In §2, we recall some facts concerning lattices in a field of series and prove a key theorem from which the rest of our results will follow. Section 3 gives a precise statement of the k-distribution problem that we want to address. We solve that problem in §4 for the case of an irreducible modulus m and in §5 for the case of combined generators with two or three components. In all cases, we assume (among other things) that a and m are polynomials in K and that the generator has (full) period $2^p - 1$, where p is the degree of m. Section 6 (in the Supplements section at the end of this issue) gives numerical examples illustrating the practical implications of our results.

2. Lattices

Following Mahler [6], we define a non-Archimedean valuation in K by

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ 2^n & \text{if } x \neq 0 \text{ and } x \text{ is given by (1) with } \alpha_n \neq 0. \end{cases}$$

This makes K a locally compact field. Let k denote a positive integer. The vector space K^k is then normed by $\|X\| = \max_{1 \le i \le k} |x_i|$, where $X = (x_1, \ldots, x_k)$, and it is also locally compact.

We now consider, in K, the subring of polynomials $A = \mathbb{F}_2[z]$ and A-submodules of K^k. We call one such submodule a *lattice* if it is discrete in K^k. We will not assume, as is usually done, that a lattice has maximal rank over A. One may then define its rank as the dimension of the K-vector subspace it generates. We note that, because of local compactness, linear independence in a lattice is the same over A as over K. We will make use of the following result (see the proof of Lemma 1 of [7]).

Theorem 1. *Let $X_1, \ldots, X_h$ be points in a lattice $L \subset K^k$ of rank h with the following properties:*

(i) *X_1 is a shortest nonzero vector in L;*

(ii) *for* $i = 2, \dots, h$, X_i *is a shortest vector among the set of vectors* X *in* L *such that* $X_1, \dots, X_{i-1}, X$ *are linearly independent over* A.

Then $X_1, \dots, X_h$ *form a basis of* L *over* A. □

Since any cube $C_r = \{X \mid \|X\| < 2^r\}$, $r \in \mathbb{Z}$, contains but a finite number of points in a given lattice L, it follows that a system as in Theorem 1 always exists. This system is a *reduced* basis for L (in the sense of Minkowski). The numbers $\sigma_i = \|X_i\| > 0$ are then uniquely determined by the lattice and are called its *successive minima.* Lenstra [4] gives details on how to compute these numbers (and a reduced basis) efficiently when the lattice is integral (i.e., contained in A^k).

One can view $L \cap C_r$ as a vector space over $\mathbb{F}_2$, with cardinality 2^d, where d is its finite dimension over $\mathbb{F}_2$. In the next theorem, we show that the number 2^d of lattice points in the cube C_r is determined by r and the lattice's successive minima. Let $s_i = \log_2 \sigma_i$ (an integer). For $t \in \mathbb{R}$, let t^+ denote $\max(t, 0)$.

Theorem 2. *One has*

$$d = \sum_{i=1}^{h} (r - s_i)^+. \tag{3}$$

Proof. Let $X_1, \dots, X_h$ be as in Theorem 1. For each integer $j \geq 0$, let $h_j = \max\{i \leq h \mid s_i \leq j\}$ be the number of points X_i contained in C_{j+1} and, for $1 \leq i \leq h_j$, let $X_i^{(j)} = z^{j-s_i} X_i$. Then, $\|X_i^{(j)}\| = 2^j$. We will now prove that the system $\mathscr{B} = \{X_i^{(j)} \mid j < r,\ 1 \leq i \leq h_j\}$ is a basis for $L \cap C_r$ over $\mathbb{F}_2$. From that, equation (3) easily follows.

We show first that for each $j \geq s_1$, the system $X_1^{(j)}, \dots, X_{h_j}^{(j)}$ is linearly independent over $\mathbb{F}_2$ modulo C_j. Let us prove that property by induction on j. For $j = s_1$, one has $h_j = \max\{i \leq h \mid s_i = s_1 = j\}$ and the vectors $X_1^{(j)}, \dots, X_{h_j}^{(j)}$ are in fact $X_1, \dots, X_{h_j}$, which are linearly independent by construction. Now, let $j \geq s_1 + 1$ and assume that $X_1^{(j-1)}, \dots, X_{h_{j-1}}^{(j-1)}$ are linearly independent over $\mathbb{F}_2$ modulo C_{j-1}. Let $X \in C_j$ be a linear combination over $\mathbb{F}_2$ of $X_1^{(j)}, \dots, X_{h_j}^{(j)}$. If $j = s_i$ for some i, let $l = \min\{i \mid s_i = j\}$. This linear combination cannot involve any of $X_l^{(j)}, \dots, X_{h_j}^{(j)}$ (that is, $X_l, \dots, X_{h_j}$), since X would be linearly independent of $X_1, \dots, X_{l-1}$ (and shorter than X_l) contradicting the minimality property of X_l. If $j \neq s_i$ for all i, then $h_j = h_{j-1}$. Therefore, in both cases, the linear combination can involve only $X_1^{(j)}, \dots, X_{h_{j-1}}^{(j)}$. For these we have $X_i^{(j)} = zX_i^{(j-1)}$ and, since multiplication by z is a linear (over $\mathbb{F}_2$) automorphism of K^k mapping C_{j-1} onto C_j, it follows that they are linearly independent over $\mathbb{F}_2$ modulo C_j and our linear combination must be trivial. This completes the induction.

We are now ready to show that $\mathscr{B}$ is a basis , i.e., that it is linearly independent and that every vector of $L \cap C_r$ can be expressed as a linear combination of vectors of $\mathscr{B}$. Let $X \in L$. From Theorem 1, X can be expressed uniquely as a linear combination of $X_1, \ldots, X_h$, with coefficients in A, that is

$$X = \sum_{i=1}^{h} \sum_{n \geq 0} c_{in} z^n X_i = \sum_{i=1}^{h} \sum_{j \geq s_i} \tilde{c}_{ij} X_i^{(j)}, \tag{4}$$

where each $c_{in} = \tilde{c}_{i,s_i+n}$ is in $\mathbb{F}_2$ and there are finitely many nonzero c_{in}'s. Since the c_{in}'s are unique, the $\tilde{c}_{in}$'s are also unique. If $X = 0$, then each c_{in} must be zero because the X_i's are independent over A. As a consequence, if $X = 0$, each $\tilde{c}_{ij}$ must be zero, which implies that $\mathscr{B}$ is linearly independent over $\mathbb{F}_2$.

It remains to show that, if $X \in C_r$, $\tilde{c}_{ij} \neq 0$ implies $j < r$. Let $l = \max\{j \mid \tilde{c}_{ij} \neq 0\}$. One has $l \geq s_1$, because $s_1 \leq s_2 \leq \cdots \leq s_k$ and the sum in (4) is extended over $j \geq s_i$. Suppose that $l \geq r$, and let

$$\widetilde{X} = \sum_{i=1}^{h} \tilde{c}_{il} X_i^{(l)} = X - \sum_{i=1}^{h} \sum_{j=s_i}^{l-1} \tilde{c}_{ij} X_i^{(j)}.$$

Since $X \in C_r \subseteq C_l$ and $X_i^{(j)} \in C_l$ for each $j < l$, one has $\widetilde{X} \in C_l$. In other words, $\widetilde{X} = 0$ modulo C_l. Since $X_1^{(l)}, \ldots, X_{h_l}^{(l)}$ are linearly independent modulo C_l, this implies $\tilde{c}_{il} = 0$ for each i, which contradicts the definition of l. Therefore, $l < r$ and the conclusion follows. □

3. The question of k-distribution

For the remainder of the paper, we assume given $a, m \in K$ satisfying the following assumptions:

(A1) $a, m \in A$;

(A2) The group $(A/(m))^\times$ of invertible elements of the quotient ring $A/(m)$ is cyclic and a is a generator for it;

(A3) m has no factor of the first degree. □

We consider all k-tuples of successive nontruncated terms of (2):

$$R_i = (\mathrm{frac}(a^i/m), \ldots, \mathrm{frac}(a^{i+k-1}/m)), \qquad i = 0, 1, \ldots,$$

and the A-submodule of K^k defined by

$$L = AR_0 + A^k.$$

From (A1), L is a lattice that contains all the R_i's. We call it the lattice *associated* with the pseudorandom sequence defined by a and m. The mapping $x \to \mathrm{frac}(xR_0)$, $x \in A$, where frac is applied componentwise, induces an isomorphism

$$A/(m) \simeq L \cap C_0 \tag{5}$$

and, if S is the subset of $L \cap C_0$ that corresponds to $(A/(m))^\times$, it follows from (A2) that the sequence $\{R_i,\ i = 0, 1, \ldots\}$ runs cyclically through all points of S and that each point is visited exactly once per period.

For each integer $l \geq 0$, let $E_l = \text{trunc}_l(C_0)$, where trunc_l is applied componentwise. The operator trunc_l then defines a linear transformation over $\mathbb{F}_2$,

$$\text{trunc}_l : L \cap C_0 \to E_l. \tag{6}$$

We now define a frequency function $f_l : E_l \to \mathbb{N} \cup \{0\}$ by

$$f_l(X) = \text{card}\{R \in S \mid \text{trunc}_l(R) = X\}.$$

The set E_l corresponds to a partition of the hypercube $[0, 1)^k$ into 2^{lk} cubic cells of the same size; we note that, if $X \in E_l$ and $R \in S$, the condition $\text{trunc}_l(R) = X$ means that the point in $\mathbb{R}^k$ corresponding to R lies (strictly, because of (A3)) inside the cube $\prod_{i=1}^{k}[x_i, x_i + 2^{-l})$, where x_i is the real number corresponding to the ith coordinate of X; $f_l(X)$ is then the number of such points $R \in S$ falling into this cube. For each integer n, let

$$\varphi_l(n) = \text{card}\{X \in E_l \mid f_l(X) = n\},$$

which represents the number of cells that contain exactly n points. We will be concerned in the next sections with the problem of computing $\varphi_l(n)$ efficiently for every nonnegative integer n.

4. Simple generators

We first consider the case where the polynomial m is irreducible. In that case, the pseudorandom sequence is called *simple.* Let p be the degree of m. From (5) we see that $S = L \cap C_0 \setminus \{0\}$. Also, the kernel of the mapping (6) is $L \cap C_{-l}$ and, if we denote its image by $L^{(l)}$, we obtain for $X \in E_l$,

$$f_l(X) = \begin{cases} 0 & \text{if } X \in E_l \setminus L^{(l)}, \\ \text{card}(L \cap C_{-l}) & \text{if } X \in L^{(l)} \setminus \{0\}, \\ \text{card}(L \cap C_{-l}) - 1 & \text{if } X = 0. \end{cases}$$

Now, $\text{card}(L \cap C_{-l}) = 2^d$, where d is given in Theorem 2 with $r = -l$ and $h = k$. Then, from (6) and (5), $\dim_{\mathbb{F}_2}(L^{(l)}) = \dim_{\mathbb{F}_2}(L \cap C_0) - d = p - d$. Since $\dim_{\mathbb{F}_2}(E_l) = kl$, there are $2^{kl} - 2^{p-d}$ points in $E_l \setminus L^{(l)}$ and 2^{p-d} points in $L^{(l)}$. This is summarized in Table 1, which gives the value of $\varphi_l(n)$ for all values of n for which it could be nonzero.

Tezuka [12] calls the pseudorandom sequence k-distributed with resolution l when the case $n = 0$ does not occur, i.e., when

$$lk = p - d. \tag{7}$$

In the trivial case $l = 0$, we have $E_l = \{0\}$ and $d = p$, so that (7) holds. As l increases through successive integers, $r = -l$ correspondingly decreases and

Table 1. Values of $\varphi_l(n)$ that could be nonzero

n	$\varphi_l(n)$
2^d	$2^{p-d} - 1$
$2^d - 1$	1
0	$2^{lk} - 2^{p-d}$

by Theorem 2, (7) remains valid if and only if $r \geq \log \sigma_k$ (note that $\log \sigma_k \leq 0$ since $A^k \subset L$). This gives another proof of the following result of Tezuka [12, Theorem 1]:

Corollary 1. *A simple pseudorandom sequence in K defined by a and (irreducible) m is k-distributed with resolution l if and only if* $\log \sigma_k \leq -l$. □

5. Combined generators with J simple components

5.1. **General formulae.** We consider now the case where m is a product of J irreducible factors, $m = m_1 \cdots m_J$, where for each j, $p_j \geq 2$ is the degree of m_j and $p = p_1 + \cdots + p_J$ is the degree of m. Assumptions (A1)–(A3) then hold, provided that for each pair $i \neq j$, $\mathrm{GCD}(2^{p_i} - 1, \; 2^{p_j} - 1) = 1$. For $j = 1, \ldots, J$, let L_j be the lattice in K^k associated with the LS2 sequence defined by (a, m_j).

By the Chinese Remainder theorem, we have a ring isomorphism

$$A/(m_1) \times \cdots \times A/(m_J) \simeq A/(m). \tag{8}$$

Through (5), this becomes

$$L \cap C_0 = (L_1 \cap C_0) \oplus \cdots \oplus (L_J \cap C_0) \tag{9}$$

(direct sum of vector spaces over $\mathbb{F}_2$). For each j, define $V_j = L_j \cap C_0$. For each subset Ψ of $\{1, \ldots, J\}$, define $m_\Psi = \prod_{j \in \Psi} m_j$, $V_\Psi = \bigoplus_{j \in \Psi} V_j$, $W_\Psi = V_\Psi \cap C_{-l}$, and $d_\Psi = \dim(W_\Psi)$. If $\Psi = \{1, \ldots, J\}$, we also write V_Ψ and W_Ψ as V and W respectively. (Note that all objects and quantities defined above depend implicitly on k and l.) Each d_Ψ can be computed using (3) in Theorem 2, with $r = -l$, $h = k$, and $L = L_\Psi$, where L_Ψ is the lattice associated with the LS2 sequence defined by (a, m_Ψ). Then,

$$S = V \Big\backslash \bigcup_{|\Psi| = J-1} V_\Psi. \tag{10}$$

For each $X \in E_l \setminus L^{(l)}$, one has $f_l(X) = 0$. Those $X \in L^{(l)}$ correspond by (6) to the cosets W' of W in V. For any given coset W', we define the *signature* of W' (also the signature of X) as the set $\Phi(W') = \{\Psi \subseteq \{1, \ldots, J\} \mid W' \cap V_\Psi \neq \varnothing\}$. Observe that for each W', $\mathrm{card}(W') = \mathrm{card}(W) = 2^d$ and when W' intersects V_Ψ, $\mathrm{card}(W' \cap V_\Psi) = \mathrm{card}(W \cap V_\Psi) = \mathrm{card}(W_\Psi) = 2^{d_\Psi}$. A nonempty family Φ of subsets of $\{1, \ldots, J\}$ such that $\Psi \in \Phi$ and $\Psi \subset \Psi'$ imply $\Psi' \in \Phi$, will be called a *maximal family*. Reciprocally, a nonempty family Γ of subsets of $\{1, \ldots, J\}$ such that $\Psi_1, \Psi_2 \in \Gamma$ implies $\Psi_1 \not\subset \Psi_2$ and $\Psi_2 \not\subset \Psi_1$, will be called a *minimal family*. Let Ω and Δ denote the classes of all maximal and minimal families, respectively. A set Ψ belonging to a maximal family Φ is called a *minimal element* of Φ if no proper subset of Ψ belongs to Φ. The set of minimal elements of Φ will be called the *generator* of Φ, and denoted by $\tau(\Phi)$. Since $\tau(\Phi)$ contains only minimal elements, it is clearly a minimal family, that is, $\tau(\Phi) \in \Delta$. The next lemma shows that the mapping $\tau : \Omega \to \Delta$ is one-to-one and onto, and also that Ω contains all signatures.

Lemma 1. *If Φ is a signature, then $\Phi \in \Omega$. Also, $\tau : \Omega \to \Delta$ is one-to-one and onto.*

Proof. Let $\Phi = \Phi(W')$ be a signature and assume $\Psi \in \Phi$. Then $W' \cap V_\Psi \neq \varnothing$ and, if $\Psi \subset \Psi'$, V_Ψ is a subset of $V_{\Psi'}$ and $W' \cap V_{\Psi'} \neq \varnothing$. Therefore $\Phi \in \Omega$. Now, let $\Gamma \in \Delta$ and let Φ be the family of all subsets of $\{1, \dots, J\}$ that contain (or are equal to) some element of Γ. Then, $\Phi \in \Omega$ and $\tau(\Phi) = \Gamma$, which proves that τ is onto. If Φ_1 is another maximal family with $\tau(\Phi_1) = \Gamma$, then $\Phi \subseteq \Phi_1$, because $\Gamma \subseteq \Phi_1$, so that by the definition of Φ and since $\Phi_1 \in \Omega$, every set of Φ must be in Φ_1. Also, since $\tau(\Phi_1) = \Gamma$, all sets of $\Phi_1 \setminus \Gamma$ have proper subsets in Γ, which implies that $\Phi_1 \subseteq \Phi$. Therefore, one must have $\Phi_1 = \Phi$, which means that τ is one-to-one. □

Let $X \in L^{(l)}$, and let W' be the coset that is mapped to X. We then have, from (10) and using a standard inclusion-exclusion argument,

$$\begin{aligned} f_l(X) = \operatorname{card}(W' \cap S) &= \sum_{i=0}^{J} (-1)^i \sum_{|\Psi| = J-i} \operatorname{card}(W' \cap V_\Psi) \\ &= \sum_{\Psi \in \Phi(W')} (-1)^{J-|\Psi|} 2^{d_\Psi}. \end{aligned} \tag{11}$$

For each $\Phi \in \Omega$, let c_Φ denote the number of cosets of W (in V) with signature Φ. In view of (11), it will be sufficient to determine these numbers. We will use intermediate quantities

$$C_\Gamma = \operatorname{card}\left(\left(\bigcap_{\Psi \in \Gamma} (V_\Psi + W)\right) \bigg/ W\right), \qquad \Gamma \in \Delta. \tag{12}$$

The quantity C_Γ is the number of cosets W' with signature $\Phi \supseteq \tau^{-1}(\Gamma)$, that is, with the property that $W' \cap V_\Psi \neq \varnothing$ if and only if $\Psi \in \Phi$. They are related to the c_Φ's by the equations

$$\sum_{\{\Phi | \Gamma \subseteq \Phi\}} c_\Phi = C_\Gamma, \qquad \Gamma \in \Delta. \tag{13}$$

Observe that the sum in (13) is over all maximal families Φ that contain $\tau^{-1}(\Gamma)$. The quantities C_Γ will be determined, partly by Theorem 3, and completely in cases $J = 2$ or 3. In such cases, one can also compute the c_Φ's using (13) because of the following lemma.

Lemma 2. *The linear system* (13) *admits a unique solution* c_Φ, $\Phi \in \Omega$, *for any given set of values for the* C_Γ*'s.*

Proof. Since Ω and Δ have the same cardinality by Lemma 1, it is sufficient to show that all c_Φ's are 0 if all C_Γ's are 0. Suppose $C_\Gamma = 0$ for each $\Gamma \in \Delta$. For each maximal family Φ, let s_Φ denote the number of maximal families that contain Φ. We proceed by induction on s_Φ. If $s_\Phi = 1$ then, for $\Gamma = \tau(\Phi)$, the sum in (13) has only one term, namely c_Φ, which must be zero. Now, let $s > 1$ and assume that $c_\Phi = 0$ whenever $s_\Phi < s$. Let Φ be a maximal family such that $s_\Phi = s$. For any maximal family Φ' that contains Φ strictly, one must have $s_{\Phi'} < s_\Phi = s$, and therefore $c_{\Phi'} = 0$. Then, c_Φ is the only possible nonzero term that remains in the sum in (13) for $\Gamma = \tau(\Phi)$. Since that sum is zero, c_Φ must be zero. This completes the induction. □

For each $\Gamma \in \Delta$, we define

$$\gamma(\Gamma) = \dim\left(\bigcap_{\Psi\in\Gamma}(V_\Psi + W)\right) - \dim(W), \tag{14}$$

so that

$$C_\Gamma = 2^{\gamma(\Gamma)}. \tag{15}$$

Theorem 3. *Let $\Gamma \in \Delta$ and $\Psi_0 = \bigcup_{\Psi\in\Gamma}\Psi$. If the canonical mapping*

$$V_{\Psi_0} \to \prod_{\Psi\in\Gamma}(V_{\Psi_0}/(V_\Psi + W_{\Psi_0})) \tag{16}$$

is onto, then

$$\gamma(\Gamma) = (p_{\Psi_0} - d_{\Psi_0})(1 - |\Gamma|) + \sum_{\Psi\in\Gamma}(p_\Psi - d_\Psi). \tag{17}$$

This will be the case if $|\Gamma| = 1$ or 2. If the mapping is not onto, "=" must be replaced by " $\geq$ " in (17).

Proof. The canonical mapping (16) has kernel $\bigcap_{\Psi\in\Gamma}(V_\Psi + W_{\Psi_0})$. But the dimension of V_{Ψ_0} must be equal to the dimension of the kernel plus the dimension of the image. That is, if the mapping is onto,

$$p_{\Psi_0} = \dim(V_{\Psi_0}) = \dim\left(\bigcap_{\Psi\in\Gamma}(V_\Psi + W_{\Psi_0})\right) + \sum_{\Psi\in\Gamma}\dim(V_{\Psi_0}/(V_\Psi + W_{\Psi_0})).$$

Observe that

$$\begin{aligned}\dim(V_{\Psi_0}/(V_\Psi + W_{\Psi_0})) &= \dim(V_{\Psi_0}) - (\dim(V_\Psi) + \dim(W_{\Psi_0}) - \dim(V_\Psi \cap W_{\Psi_0}))\\ &= p_{\Psi_0} - d_{\Psi_0} - p_\Psi + d_\Psi\end{aligned}$$

and that the canonical mapping

$$\bigcap_{\Psi\in\Gamma}(V_\Psi + W_{\Psi_0})/W_{\Psi_0} \to \bigcap_{\Psi\in\Gamma}(V_\Psi + W)/W \tag{18}$$

is an isomorphism. Then,

$$\begin{aligned}\dim\left(\bigcap_{\Psi\in\Gamma}(V_\Psi + W)/W\right) &= \dim\left(\bigcap_{\Psi\in\Gamma}(V_\Psi + W_{\Psi_0})/W_{\Psi_0}\right)\\ &= \dim\left(\bigcap_{\Psi\in\Gamma}(V_\Psi + W_{\Psi_0})\right) - \dim(W_{\Psi_0})\\ &= p_{\Psi_0} - d_{\Psi_0} - \sum_{\Psi\in\Gamma}(p_{\Psi_0} - d_{\Psi_0} - p_\Psi + d_\Psi)\\ &= (1 - |\Gamma|)(p_{\Psi_0} - d_{\Psi_0}) + \sum_{\Psi\in\Gamma}(p_\Psi - d_\Psi).\end{aligned}$$

If the mapping is not onto, the second equality in this proof must be replaced by $\leq$ and the next to last equality above must be replaced by $\geq$.

If $|\Gamma| = 1$, say $\Gamma = \{\Psi\}$, then (16) becomes $V_\Psi \to V_\Psi/(V_\Psi + W_\Psi)$, which is clearly onto. Suppose that $|\Gamma| = 2$, namely $\Gamma = \{\Psi_1, \Psi_2\}$. Let $\tilde{v} = (\tilde{v}_2, \tilde{v}_1) \in V_{\Psi_0}/(V_{\Psi_1} + W_{\Psi_0}) \times V_{\Psi_0}/(V_{\Psi_2} + W_{\Psi_0})$. Since $V_{\Psi_0} = V_{\Psi_1} + V_{\Psi_2}$, there is a $v_2 \in V_{\Psi_2} \cap \tilde{v}_2$, and similarly for v_1. Then, $v = v_1 + v_2 \in V_{\Psi_0}$ is mapped to $\tilde{v}$. So, the mapping (16) is again onto. □

Below, we give specific tables for the cases $J = 2$ and $J = 3$. For $J = 2$ all the c_Φ's can be computed easily from Theorem 3. For $J = 3$, Theorem 3 gives us one equation for each set $\Gamma \in \Delta$, except for one, for which the mapping (16) is not onto. We obtain this last equation and show how all the c_Φ's can be computed by considering a special lattice, different from the L_Ψ's, and its successive minima. Below, Φ denotes the signature of X.

5.2. **Two simple components.** For $J = 2$, we have card$(\Omega) = 5$ as shown in Table 2. We number these signatures from 1 to 5 and, to simplify the notation, we will replace each signature Φ by its corresponding number when used as a subscript of c. In this case, Theorem 3 gives us an equation for each set Γ, as shown in Table 3.

TABLE 2. Possible signatures and frequencies for generators with two components

n	Φ	$f_l(X)$
1	$\{\{1, 2\}\}$	2^d
2	$\{\{1, 2\}, \{1\}\}$	$2^d - 2^{d_1}$
3	$\{\{1, 2\}, \{2\}\}$	$2^d - 2^{d_2}$
4	$\{\{1, 2\}, \{1\}, \{2\}\}$	$2^d - 2^{d_1} - 2^{d_2}$
5	$\{\{1, 2\}, \{1\}, \{2\}, \phi\}$	$2^d - 2^{d_1} - 2^{d_2} + 1$

TABLE 3. Equations given by Theorem 3, for $J = 2$

Γ	equation
$\{\{1, 2\}\}$	$c_1 + c_2 + c_3 + c_4 + c_5 = 2^{p-d}$
$\{\{1\}\}$	$c_2 + c_4 + c_5 = 2^{p_1-d_1}$
$\{\{2\}\}$	$c_3 + c_4 + c_5 = 2^{p_2-d_2}$
$\{\{1\}, \{2\}\}$	$c_4 + c_5 = 2^{d-d_1-d_2}$
$\{\phi\}$	$c_5 = 1$

Solving the equations of Table 3, one obtains

$$\begin{aligned}
c_5 &= 1,\\
c_4 &= 2^{d-d_1-d_2} - 1,\\
c_3 &= 2^{p_2-d_2} - 2^{d-d_1-d_2},\\
c_2 &= 2^{p_1-d_1} - 2^{d-d_1-d_2},\\
c_1 &= 2^{p-d} + 2^{d-d_1-d_2} - 2^{p_1-d_1} - 2^{p_2-d_2}.
\end{aligned}$$

These results are summarized in Table 4, where the first column gives all possible values of n for which $\varphi_l(n)$ is not always zero. The integers d, d_1

TABLE 4. Values of $\varphi_l(n)$ that could be nonzero, for $J = 2$

n	$\varphi_l(n)$
2^d	$2^{p-d} + 2^{d-d_1-d_2} - 2^{p_1-d_1} - 2^{p_2-d_2}$
$2^d - 2^{d_1}$	$2^{p_1-d_1} - 2^{d-d_1-d_2}$
$2^d - 2^{d_2}$	$2^{p_2-d_2} - 2^{d-d_1-d_2}$
$2^d - 2^{d_1} - 2^{d_2}$	$2^{d-d_1-d_2} - 1$
$2^d - 2^{d_1} - 2^{d_2} + 1$	1
0	$2^{lk} - 2^{p-d}$

and d_2 are obtained from Theorem 2 applied to L, L_1, and L_2, respectively, with $r = -l$. (Note that the fourth entry of the first column in Table 4 might be equal to -1, but that then the corresponding entry in the second column is zero.) To have the points "well distributed" among the cells, one would like to have first the smallest possible d, then the smallest d_1 and d_2. The best case is $d = p - lk$ and $d_1 = d_2 = 0$, which could occur only when $lk \leq p$.

5.3. **Three simple components.** For $J = 3$, we have $\text{card}(\Omega) = 19$ as shown in Table 5. Again, we number these signatures from 1 to 19 and use these numbers as subscripts of c.

For all those minimal families Γ whose cardinality is 1 or 2, Theorem 3 yields C_Γ directly. For $\Gamma = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, it can be verified that the mapping (16) is onto, so that Theorem 3 applies. Indeed, let $\tilde{v} = (\tilde{v}_3, \tilde{v}_2, \tilde{v}_1) \in (V/(V_{12} + W)) \times (V/(V_{13} + W)) \times (V/(V_{23} + W))$. Since $V = V_{12} + V_3$, there is a $v_3 \in V_3 \cap \tilde{v}_3$, and similarly for v_2 and v_1. Then, $v = v_1 + v_2 + v_3 \in V$ is mapped to $\tilde{v}$ by (16). There remains the case $\Gamma = \{\{1\}, \{2\}, \{3\}\}$, which

TABLE 5. Possible signatures and frequencies for generators with three components

n	Φ	$f_l(X)$
1	$\{\{1, 2, 3\}\}$	2^d
2	$\{\{1, 2, 3\}, \{1, 2\}\}$	$2^d - 2^{d_{12}}$
3	$\{\{1, 2, 3\}, \{1, 3\}\}$	$2^d - 2^{d_{13}}$
4	$\{\{1, 2, 3\}, \{2, 3\}\}$	$2^d - 2^{d_{23}}$
5	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}}$
6	$\{\{1, 2, 3\}, \{1, 2\}, \{2, 3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{23}}$
7	$\{\{1, 2, 3\}, \{1, 3\}, \{2, 3\}\}$	$2^d - 2^{d_{13}} - 2^{d_{23}}$
8	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}}$
9	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{1\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} + 2^{d_1}$
10	$\{\{1, 2, 3\}, \{1, 2\}, \{2, 3\}, \{2\}\}$	$2^d - 2^{d_{12}} - 2^{d_{23}} + 2^{d_2}$
11	$\{\{1, 2, 3\}, \{1, 3\}, \{2, 3\}, \{3\}\}$	$2^d - 2^{d_{13}} - 2^{d_{23}} + 2^{d_3}$
12	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_1}$
13	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{2\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_2}$
14	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_3}$
15	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_1} + 2^{d_2}$
16	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_1} + 2^{d_3}$
17	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{2\}, \{3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_2} + 2^{d_3}$
18	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_1} + 2^{d_2} + 2^{d_3}$
19	$\{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}, \phi\}$	$2^d - 2^{d_{12}} - 2^{d_{13}} - 2^{d_{23}} + 2^{d_1} + 2^{d_2} + 2^{d_3} - 1$

TABLE 6. Equations given by Theorem 3 for $J = 3$

Γ	equation		
$\{\{1,2,3\}\}$	$c_1 + c_2 + \cdots + c_{19}$	=	2^{p-d}
$\{\{1,2\}\}$	$c_2 + c_5 + c_6 + c_8 + c_9 + c_{10} + c_{12} + \cdots + c_{19}$	=	$2^{p_{12}-d_{12}}$
$\{\{1,3\}\}$	$c_3 + c_5 + c_7 + c_8 + c_9 + c_{11} + c_{12} + \cdots + c_{19}$	=	$2^{p_{13}-d_{13}}$
$\{\{2,3\}\}$	$c_4 + c_6 + c_7 + c_8 + c_{10} + c_{11} + c_{12} + \cdots + c_{19}$	=	$2^{p_{23}-d_{23}}$
$\{\{1,2\},\{1,3\}\}$	$c_5 + c_8 + c_9 + c_{12} + \cdots + c_{19}$	=	$2^{p_1+d-d_{12}-d_{13}}$
$\{\{1,2\},\{2,3\}\}$	$c_6 + c_8 + c_{10} + c_{12} + \cdots + c_{19}$	=	$2^{p_2+d-d_{12}-d_{23}}$
$\{\{1,3\},\{2,3\}\}$	$c_7 + c_8 + c_{11} + c_{12} + \cdots + c_{19}$	=	$2^{p_3+d-d_{13}-d_{23}}$
$\{\{1,2\},\{1,3\},\{2,3\}\}$	$c_8 + c_{12} + \cdots + c_{19}$	=	$2^{2d-d_{12}-d_{13}-d_{23}}$
$\{\{2,3\},\{1\}\}$	$c_{12} + c_{15} + c_{16} + c_{18} + c_{19}$	=	$2^{d-d_1-d_{23}}$
$\{\{1,3\},\{2\}\}$	$c_{13} + c_{15} + c_{17} + c_{18} + c_{19}$	=	$2^{d-d_2-d_{13}}$
$\{\{1,2\},\{3\}\}$	$c_{14} + c_{16} + c_{17} + c_{18} + c_{19}$	=	$2^{d-d_3-d_{12}}$
$\{\{1\}\}$	$c_9 + c_{12} + c_{15} + c_{16} + c_{18} + c_{19}$	=	$2^{p_1-d_1}$
$\{\{2\}\}$	$c_{10} + c_{13} + c_{15} + c_{17} + c_{18} + c_{19}$	=	$2^{p_2-d_2}$
$\{\{3\}\}$	$c_{11} + c_{14} + c_{16} + c_{17} + c_{18} + c_{19}$	=	$2^{p_3-d_3}$
$\{\{1\},\{2\}\}$	$c_{15} + c_{18} + c_{19}$	=	$2^{d_{12}-d_1-d_2}$
$\{\{1\},\{3\}\}$	$c_{16} + c_{18} + c_{19}$	=	$2^{d_{13}-d_1-d_3}$
$\{\{2\},\{3\}\}$	$c_{17} + c_{18} + c_{19}$	=	$2^{d_{23}-d_2-d_3}$
$\{\{1\},\{2\},\{3\}\}$	$c_{18} + c_{19}$	=	2^D
$\{\phi\}$	c_{19}	=	1

is more difficult and is taken care of by Lemma 3 below. These results are summarized in Table 6. From the equations of Table 6, the c_i's (i.e., the values of $\varphi_I(n)$) can be computed easily.

We now explain how to deal with $\Gamma = \{\{1\},\{2\},\{3\}\}$, i.e., how to compute $D = \dim(((V_1 + W) \cap (V_2 + W) \cap (V_3 + W))/W)$. For this case, the mapping (16) is not onto in general and D cannot be determined by only the p_Φ's and d_Φ's. We give examples of that at the end of the Appendix. Consider the lattice $L' = L_{12} \times L_{13} \times L_{23} \subset K^{3k}$ and the mapping η: $K^{3k} \mapsto K^k$ defined by $\eta(v_1, v_2, v_3) = v_1 + v_2 + v_3$. Let $\overline{L} = L' \cap \ker(\eta) = \{v \in L' \mid \eta(v) = 0\}$, the kernel of η restricted to L'. This $\overline{L}$ is a lattice in K^{3k} and we have:

Lemma 3. $D = \dim(\overline{L} \cap C_{-l}) - d_1 - d_2 - d_3$.

Proof. Let $\overline{W} = W_{12} + W_{13} + W_{23}$ and $\overline{d} = \dim(\overline{W})$. From Lemma 6 in the Appendix (in the Supplement section), one has

$$D = d_{12} + d_{13} + d_{23} - d_1 - d_2 - d_3 - \overline{d}. \tag{19}$$

But since $\eta(W_{12} \times W_{13} \times W_{23}) = \overline{W}$, one has

$$\begin{aligned} \dim(\overline{L} \cap C_{-l}) &= \dim(\ker(\eta) \cap (W_{12} \times W_{13} \times W_{23})) \\ &= \dim(W_{12} \times W_{13} \times W_{23}) - \dim(\overline{W}) \qquad (20) \\ &= d_{12} + d_{13} + d_{23} - \overline{d}. \end{aligned}$$

Merging (19) and (20) completes the proof. □

We can now compute D using Theorem 2 by determining $\overline{L}$'s successive minima. For this, we must construct a basis for $\overline{L}$, which can then be reduced by Lenstra's algorithm [4].

We first find a set of vectors that generate $\overline{L}$. An element of L' can be written as $v = (v_1 + v_2, v_1' + v_3', v_2'' + v_3'')$ with $v_1, v_1' \in L_1$, $v_2, v_2'' \in L_2$, and $v_3', v_3'' \in L_3$. Such a v belongs to $\overline{L}$ if and only if

$$v_1 + v_1' + v_2 + v_2'' + v_3' + v_3'' = 0. \tag{21}$$

We will now work in L modulo A^k, i.e., in the quotient group L/A^k. In that group, L is the direct sum of L_1, L_2, and L_3. This comes from (9) and noticing that the mapping "frac" induces a projection $L \to L \cap C_0$ with kernel A^k (and the same for L_1, L_2 and L_3). So, from (21) we obtain $v_1 + v_1' = v_2 + v_2'' = v_3' + v_3'' = 0$ modulo A^k, and v can be written as $(v_1 + v_2, -v_1 + v_3, -v_2 - v_3) = (v_1, -v_1, 0) + (v_2, 0, -v_2) + (0, v_3, -v_3)$ (each term $\in \overline{L}$) plus something in A^{3k} which must also be in $\overline{L}$. So, a generating system for $\overline{L}$ is obtained as the union of a basis for $A^{3k} \cap \ker(\eta)$, $\{(v_1, -v_1, 0)\}$, $\{(v_2, 0, -v_2)\}$, and $\{(0, v_3, -v_3)\}$, where v_1, v_2 and v_3 run through a basis of L_1, L_2, and L_3, respectively. Finally, a basis for $A^{3k} \cap \ker(\eta)$ is given by $\{e_i - e_{i+k}, e_i - e_{i+2k} \mid i = 1, \dots, k\}$, where $e_i \in A^{3k}$ is the vector with all components 0 with the exception of the ith one, which is the polynomial equal to 1.

It now remains to transform this generating system into a basis for $\overline{L}$. This is similar to the corresponding problem for lattices in $\mathbb{R}^n$, but now, integral linear combination means a linear combination with coefficients in A. So, let $X_1, \dots, X_n$ denote a generating system, each vector having been multiplied by the modulus m so that all coordinates now belong to A. If some of these X_i's have a nonzero first coordinate, one may construct, by the usual process of finding a gcd, a linear combination of them, say X, with the property that the first coordinate of X divides (in A) the first coordinate of each X_i. One can then, by adding an integral multiple of X to the X_i's, modify them so that their first coordinate is 0. We now have a new generating system formed by the modified X_i's, together with X. In case all X_i's had zero first coordinate from the start, we just do nothing at this step. Then, we repeat the process for the second coordinate of the X_i's, etc., each time obtaining possibly a new X. At each step, the X_i's, together with all the obtained X's, still form a generating system for $\overline{L}$. Once the process is terminated for all coordinates, all the X_i's are zero and we can forget them. The basis is then the set of X's divided by the modulus m.

Bibliography

1. D. L. André, G. L. Mullen, and H. Niederreiter, *Figures of merit for digital multistep pseudorandom numbers*, Math. Comp. **54** (1990), 737–748.

2. D. E. Knuth, *The art of computer programming: seminumerical algorithms*, vol. 2, 2nd ed., Addison-Wesley, Reading, MA, 1981.

3. P. L'Ecuyer, *Random numbers for simulation*, Comm. ACM, **33**, no. 10 (1990), 85–97.

4. A. K. Lenstra, *Factoring multivariate polynomials over finite fields*, J. Comput. System Sci. **30** (1985), 235-248.

5. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, Cambridge, 1986.

→ K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series*, Ann. of Math. (2) **42** (1941), 488–522.

7. K. Mahler, *On a theorem in the geometry of numbers in a space of Laurent series*, J. Number Theory **17** (1983), 403-416.

8. G. Marsaglia et al., *The McGill random number package super-duper*, School of Computer Science, McGill University, Montreal, 1972.

9. G. L. Mullen and H. Niederreiter, *Optimal characteristic polynomials for digital multistep pseudorandom numbers*, Computing **39** (1987), 155–163.

10. H. Niederreiter, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345.

11. R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two*, Math. Comp. **19** (1965), 201–209.

12. S. Tezuka, *Random number generation based on the polynomial arithmetic modulo two*, Report no. RT-0017, IBM Research, Tokyo Research Laboratory, Oct. 1989.

13. S. Tezuka and P. L'Ecuyer, *Efficient and portable combined Tausworthe random number generators*, ACM Trans. Model. Comput. Simulation **1** (1991) 99–112.

Département d'Informatique, Université Laval, Ste-Foy, Québec, Canada G1K 7P4

Département d'IRO, Université de Montréal, C.P. 6128, Succ. A, Montréal, Québec, Canada H3C 3J7

IBM Research, Tokyo Research Laboratory, 5-19 Sanbancho, Chiyodaku, Tokyo 102, Japan
E-mail address: tezuka@trlvm.vnet.ibm.com