# Polynomial Integration Lattices

Pierre L'Ecuyer

Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succ. Centre-Ville
Montréal (Québec), H3C 3J7, Canada
lecuyer@iro.umontreal.ca

**Summary.** Lattice rules are quasi-Monte Carlo methods for estimating large-dimensional integrals over the unit hypercube. In this paper, after briefly reviewing key ideas of quasi-Monte Carlo methods, we give an overview of recent results, generalize some of them, and provide new results, for lattice rules defined in spaces of polynomials and of formal series with coefficients in the finite ring $\mathbb{Z}_b$. Some of the results are proved only for the case where $b$ is a prime (so $\mathbb{Z}_b$ is a finite field). We discuss basic properties, implementations, a randomized version, and quality criteria (i.e., measures of uniformity) for selecting the parameters. Two types of polynomial lattice rules are examined: dimensionwise lattices and resolutionwise lattices. These rules turn out to be special cases of digital net constructions, which we reinterpret as yet another type of lattice in a space of formal series. Our development underlines the connections between integration lattices and digital nets.

## 1 Introduction

Monte Carlo and quasi-Monte Carlo methods are often used for estimating integrals of the form

$$\mu = \int_{[0,1)^s} f(\mathbf{u}) d\mathbf{u}. \tag{1}$$

The basic idea is to estimate $\mu$ by

$$Q_n = \frac{1}{n} \sum_{i=0}^{n-1} f(\mathbf{u}_i), \tag{2}$$

the average of values of $f$ at the $n$ points of a set $P_n = \{\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}\} \subset [0,1)^s$. The *integration error* is then $E_n = Q_n - \mu$. It is not a serious restriction to assume that the integration domain is the $s$-dimensional unit hypercube, because most simulations whose aim is to estimate a mathematical expectation fit this framework if we view $\mathbf{u}$ as the vector of uniform random numbers that drive the simulation [18].

For the *Monte Carlo* method, the points of $P_n$ are independent random vectors uniformly distributed over $[0,1)^s$. Then, $\mathrm{E}[Q_n] = \mu$, $\mathrm{Var}[Q_n] = \sigma^2/n$ where

$$\sigma^2 = \int_{[0,1)^s} f^2(\mathbf{u}) d\mathbf{u} - \mu^2, \tag{3}$$

and, from the central-limit theorem, the size of a confidence interval on $\mu$ at a fixed level converges as $O(\sigma/\sqrt{n})$ when $n \to \infty$. *Quasi-Monte Carlo* methods use point sets $P_n$ *more evenly* spread over $[0,1)^s$ than typical random points. *Digital nets* and *integration lattices* are the two main classes of methods for constructing such point sets. [13, 18, 27, 30, 31].

For an ordinary *lattice rule*, $P_n = L_s \cap [0,1)^s$, where $L_s$ is an *integration lattice* in $\mathbb{R}^s$, i.e., a discrete subset of $\mathbb{R}^s$ closed under addition and subtraction, and such that $\mathbb{Z}^s \subset L_s$.

To define a *polynomial integration lattice* and a *polynomial lattice rule* (PLR), we replace $\mathbb{R}$ and $\mathbb{Z}$ in the above definition by the ring $\mathbb{L}_b$ of formal Laurent series with coefficients in $\mathbb{Z}_b$ and by the ring $\mathbb{Z}_b[z]$ of polynomials with coefficients in $\mathbb{Z}_b$, respectively, where $b$ is an arbitrary integer larger than 1 and $\mathbb{Z}_b$ is the ring of integers modulo $b$. An output mapping $\varphi : \mathbb{L}_b \to \mathbb{R}$ is defined in a natural way: replace the formal variable $z$ in the series by the integer $b$ and evaluate. The point set $P_n$ is then defined as the intersection of $[0,1)^s$ with the image of the lattice by $\varphi$. As we shall see later, at least for prime $b$, such point sets turn out to be special cases of digital nets, defined as follows [18, 27, 34].

Let $\mathbf{C}^{(1)}, \ldots, \mathbf{C}^{(s)}$ be matrices of dimension $\infty \times k$ with elements in $\mathbb{Z}_b$, for some integers $k \geq 1$ and $b \geq 2$. They are called the *generating matrices* of the net. For $i = 0, \ldots, b^k - 1$, write $i = \sum_{\ell=0}^{k-1} a_{i,\ell} b^\ell$ and define $\mathbf{u}_i = (u_{i,1}, \ldots, u_{i,s})$ where $u_{i,j} = \sum_{\ell=1}^{\infty} u_{i,j,\ell} b^{-\ell}$ and

$$(u_{i,j,1}, u_{i,j,2}, \ldots)^T = \mathbf{C}^{(j)} (a_{i,0}, a_{i,1}, \ldots, a_{i,k-1})^T.$$

The point set $P_n = \{\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}\}$ thus obtained, with $n = b^k$, is a *digital net* over $\mathbb{Z}_b$. These $n$ points are distinct in their first $\ell$ digits iff (if and only if) the $\ell s \times k$ matrix formed by taking the first $\ell$ rows of each $\mathbf{C}^{(j)}$ has rank $k$.

Digital nets can in fact be defined over an arbitrary commutative ring $R$ of cardinality $b$, with an identity element. One simply define bijections between $R$ and $\mathbb{Z}_b$ to map the digits of the $b$-ary expansion of $i$ to elements of $R$ and to recover the $b$-ary digits of $u_{i,j}$ from elements of $R$ [14, 18, 27, 34]. A similar generalization applies to polynomial lattices as well, where the bijections from $R$ to $\mathbb{Z}_b$ can be incorporated into $\varphi$. To simplify the exposition in this paper, we will assume that $R = \mathbb{Z}_b$ and that all the bijections are the identity.

Quasi-Monte Carlo point sets are justified by a faster convergence rate of the error $E_n$. This error depends on the interplay between $P_n$ and the function $f$, so the optimal way of constructing $P_n$ depends on $f$. Convergence rates are usually studied by restricting $f$ to a specific class of functions $\mathcal{F}$.

One may consider the *worst-case* error over $\mathcal{F}$ for a deterministic $P_n$, as in the celebrated Koksma-Hlawka inequality and its generalizations, yielding error bounds of the form $|E_n| \le \|f-\mu\|\, D(P_n)$ for all $f$ in some Banach space $\mathcal{F}$ with norm $\|\cdot\|$, where $\|f-\mu\|$ measures the *variability* of $f$ and $D(P_n)$ measures the *discrepancy* (or non-uniformity) of $P_n$. For lattice rules and digital nets, one can obtain point sets $P_n$ for which $O(|E_n|) = O(D(P_n)) = O(n^{-1}(\ln n)^s)$ [27].

One may also take a *randomized* point set $P_n$ and consider the variance or mean-square error of $E_n$ with respect to this randomization, for either the worst-case $f$ in some class $\mathcal{F}$, or the average $f$ in that class. As an example, let $\mathcal{F}$ be the Sobolev class $W_{2,s}^k$ of functions on $[0,1)^s$ whose mixed partial derivatives $D^i f$ of order $|i| \le k$ satisfy $\|D^i f\|_2 \le 1$, where $\|\cdot\|_2$ denotes the Euclidean norm. An old result from Bakhvalov [1] says that $\inf_{P_n} \sup_{f\in W_{2,s}^k} (\mathrm{E}[E_n^2])^{1/2} = O(n^{-k/s-1/2})$, where the infimum is taken over all randomized point sets $P_n$. When $k/s$ is large, this is much better than the standard Monte Carlo convergence rate of $O(n^{-1/2})$.

From another viewpoint, if $\sigma^2 < \infty$, $f$ can always be decomposed as $f(\mathbf{u}) = \mu + \sum_{\phi\ne I\subseteq\{1,\ldots,s\}} f_I(\mathbf{u})$ where $f_I$ depends only on $\{u_i,\, i\in I\}$, the $f_I$'s integrate to zero and are orthogonal, and the variance decomposes as $\sigma^2 = \sum_{I\subseteq\{1,\ldots,s\}} \sigma_I^2$ where $\sigma_I^2 = \mathrm{Var}[f_I(\mathbf{U})]$ for $\mathbf{U}$ uniformly distributed over $[0,1)^s$ [10, 30]. For each set of coordinates $I$, let $P_n(I)$ denote the projection of $P_n$ over the subspace determined by $I$. If there is a set $\mathcal{J}$ of subsets of $\{1,\ldots,s\}$ of cardinality much smaller than $2^s$ and such that $\sum_{I\in\mathcal{J}} \sigma_I^2 \approx \sigma^2$, then it suffices to make sure that the integration error (or variance) is small for the $f_I$'s such that $I\in\mathcal{J}$. This can be achieved by constructing $P_n$ so that the projections $P_n(I)$ are highly uniform for all $I\in\mathcal{J}$, which is generally much easier than having *all* projections $P_n(I)$ highly uniform. As a special case, a function $f$ is said to have *effective dimension* $d$ in proportion $\rho$ in the *superposition sense* if $\sum_{|I|\le d} \sigma_I^2 \ge \rho\sigma^2$ [30]. If $\rho$ is close to 1, this means that $f$ is well approximated by a sum of $d$-dimensional (or less) functions. High-dimensional functions with *low effective dimension* are frequent. Sometimes, the most important sets $I$ contain successive indices, or a small number of nearby indices, and the function $f$ can often be modified to make this happen [5, 17]. The set $\mathcal{J}$ of important projections depends of course on the function $f$. In practice, it is usually unknown, so the (general-purpose) point sets are constructed by considering sets $\mathcal{J}$ that contain arbitrarily selected subsets $I$ of successive or nearby coordinates.

A point set $P_n$ in $[0,1)^s$ is called *fully projection-regular* [17] if for each non-empty subset $I$ of $\{1,\ldots,s\}$, $P_n(I)$ has $n$ distinct points. It is called *dimension-stationary* [20] if whenever $1\le i_1 < \ldots < i_\eta < s$ and $1\le j\le s-i_\eta$, $P_n(\{i_1,\ldots,i_\eta\}) = P_n(\{i_1+j,\ldots,i_\eta+j\})$. Restricting the search to classes of point sets having these two desirable properties can make things easier. It ensures that projections never lose points and that $P_n(I)$ depends only on the *spacings* between the indices in $I$ (this reduces the number of

projections to examine). In particular, this disqualifies naïve rectangular grids in $s \geq 2$ dimensions, because every projection in such grids has several points superposed on each other.

The remainder of this paper is organized as follows. Section 2 recalls basic properties of ordinary lattice rules. This is helpful for comparing them with their polynomial versions. The reader can consult [17, 31] for more details. PLRs with coefficients in the ring $\mathbb{Z}_b$ for an *arbitrary* $b$ are defined and studied in section 3. These PLRs generalize the PLRs of rank 1 introduced by Niederreiter [26] and studied in [27, 14]. The case where the polynomial modulus is irreducible turns out to be a special case of a construction method introduced earlier in [25] (see [27, remark 4.45]) and also examined by Tezuka [32]. We extend the definitions and part of the results of [18, 21] to an arbitrary $b$ and give new ones (e.g., in section 3.7). A significant part of our development works for an arbitrary $b$ (even if $\mathbb{Z}_b$ is not a field) because of the special form of the integration lattices considered; it would not work for *general* lattices. On the other hand, we prove a number of results via Mahler's theory for Minkowski-reduced bases in lattices over a ring of polynomials with coefficients in a finite field. These proofs are valid only for prime $b$ (the results may hold more generally but we have no proof here). In section 4, we introduce a resolutionwise version of PLRs, based on the notion of resolutionwise lattice of Tezuka [33, 34]. The links between PLRs and digital nets [14, 27] are explored in section 5, where we reinterpret a digital net as the point set of yet another form of lattice rule, defined in terms of a lattice in the space of formal series $\mathbb{L}_b$, over $\mathbb{Z}_b$. We use this interpretation to show that PLRs are actually special cases of digital nets and to generalize certain properties of PLRs to digital nets. Due to space limitations, we cannot provide detailed proofs of all the results here. Further details will appear elsewhere.

## 2 Lattice Rules in $\mathbb{R}^s$

### 2.1 Definition and basic properties

We now summarize some of the main properties of ordinary lattice rules. Consider a *lattice*

$$L_s = \left\{ \mathbf{v} = \sum_{j=1}^{s} h_j \mathbf{v}_j \text{ such that each } h_j \in \mathbb{Z} \right\},$$

where $\mathbf{v}_1, \ldots, \mathbf{v}_s \in \mathbb{R}^s$ are linearly independent over $\mathbb{R}$ and $\mathbb{Z}^s \subseteq L_s$. Under the latter condition, $L_s$ is called an *integration lattice*. The approximation of $\mu$ by $Q_n$ with the node set $P_n = L_s \cap [0,1)^s$ is a called a *lattice rule* [12, 17, 27, 31].

Let $\mathbf{V}$ be the matrix whose rows are the basis vectors $\mathbf{v}_1, \cdots, \mathbf{v}_s$ and $\mathbf{V}^{-1}$ its inverse. The columns $\mathbf{h}_1^T, \ldots, \mathbf{h}_s^T$ of $\mathbf{V}^{-1}$ form a basis of the *dual lattice*, defined as $L_s^* = \{\mathbf{h} \in \mathbb{R}^s : \mathbf{h} \cdot \mathbf{v} \in \mathbb{Z} \text{ for all } \mathbf{v} \in L_s\}$. One has $\mathbb{Z}^s \subseteq L_s$ iff

$L_s^* \subseteq \mathbb{Z}^s$ iff all entries of $\mathbf{V}^{-1}$ are integer. When this holds, $n = \det(\mathbf{V}^{-1})$ and all entries of $\mathbf{V}$ are multiples of $1/n$.

The *rank* of the lattice is the smallest $r$ such that one can find a basis of the form $\mathbf{v}_1, \ldots, \mathbf{v}_r, \mathbf{e}_{r+1}, \cdots, \mathbf{e}_s$, where $\mathbf{e}_j$ is the $j$th unit vector in $s$-dimensions. In particular, a lattice rule of *rank 1* has a basis of the form $\mathbf{v}_1 = (a_1, \ldots, a_s)/n$ and $\mathbf{v}_j = \mathbf{e}_j$ for $j > 1$, where $a_j \in \mathbb{Z}_n$ for each $j$. It is called a *Korobov* lattice rule if $\mathbf{v}_1$ has the special form $\mathbf{v}_1 = (1,\ a,\ a^2 \bmod n,\ \ldots,\ a^{s-1} \bmod n)/n$ for some $a \in \mathbb{Z}_n$. The point set $P_n$ of a Korobov lattice rule can also be written as $P_n = \{(x_1, \ldots, x_s)/n$ such that $x_1 \in \mathbb{Z}_n$ and $x_j = ax_{j-1} \bmod n$ for all $j > 1\}$, which is the set of all vectors of successive values produced by a linear congruential generator (LCG) with modulus $n$ and multiplier $a$, from all possible initial states (including 0). This gives an efficient way of enumerating $P_n$ if the LCG has full period.

The *projection* $L_s(I)$ of $L_s$ over the subspace determined by $I = \{i_1, \ldots, i_\eta\}$ is also a lattice, with point set $P_n(I)$. A rule of rank 1 is fully projection-regular iff $\gcd(n, a_j) = 1$ for all $j$, and a Korobov rule is fully projection-regular and dimension-stationary iff $\gcd(n, a) = 1$ [17].

### 2.2 Sequences of imbedded lattices

It is possible to construct sequences of lattices $L_s^1 \subset L_s^2 \subset L_s^3 \subset \ldots$, so that each lattice contains the previous one [4, 9, 11]. Such sequences permit one to increase the cardinality of $P_n$ sequentially, without throwing away the points already considered. If the point set $L_s^\xi \cap [0,1)^s$ contains $n_\xi$ points, then $n_{\xi-1}$ must divide $n_\xi$, for each $\xi$. For example, the $\xi$th rule can be a Korobov rule with $n_\xi$ points and multiplier $a_\xi$, where $a_\xi \bmod n_{\xi-1} = a_{\xi-1}$, for each $\xi$. A simple case is when $n_\xi = 2^\xi$. Then, for each $\xi$, $a_\xi = a_{\xi-1}$ or $a_\xi = a_{\xi-1} + n_{\xi-1}$.

### 2.3 Fourier expansion of $f$ and variance for randomly-shifted rules

The *Fourier expansion* of $f$ can be written as

$$f(\mathbf{u}) = \sum_{\mathbf{h} \in \mathbb{Z}^s} \hat{f}(\mathbf{h}) \exp(2\pi\sqrt{-1}\,\mathbf{h} \cdot \mathbf{u}), \tag{4}$$

with *Fourier coefficients*

$$\hat{f}(\mathbf{h}) = \int_{[0,1)^s} f(\mathbf{u}) \exp(-2\pi\sqrt{-1}\,\mathbf{h} \cdot \mathbf{u}) d\mathbf{u}.$$

If this series converges absolutely (a rather strong assumption), then the integration error with the lattice rule can be written as [31]:

$$E_n = \sum_{\mathbf{0} \neq \mathbf{h} \in L_s^*} \hat{f}(\mathbf{h}). \tag{5}$$

To obtain an unbiased estimator of $\mu$ as well as a statistical error estimate, the point set $P_n$ is often randomized. One way of doing this is the Cranley-Patterson rotation [4] (or *random shift*), defined as follows. Generate a single random point $\mathbf{U}$ uniformly over $[0,1)^s$, replace $P_n$ by $(P_n + \mathbf{U}) \bmod 1$, where the reduction modulo 1 is applied coordinatewise, and compute the corresponding $Q_n$. Repeat this $m$ times with the same $P_n$, independently, and let $\bar{X}$ and $S_x^2$ be the sample mean and variance of the $m$ corresponding values of $Q_n$. Then, $\mathrm{E}[\bar{X}] = \mu$ and $\mathrm{E}[S_x^2] = \mathrm{Var}[Q_n] = m\mathrm{Var}[\bar{X}]$, regardless of the type of point set $P_n$. Suppose $\sigma^2 < \infty$. Then, for the Monte Carlo method,

$$n\mathrm{Var}[Q_n] = \sigma^2 = \sum_{\mathbf{0}\neq\mathbf{h}\in\mathbb{Z}^s} |\hat{f}(\mathbf{h})|^2, \tag{6}$$

whereas for a randomly-shifted lattice rule [20],

$$\mathrm{Var}[Q_n] = \sum_{\mathbf{0}\neq\mathbf{h}\in L_s^*} |\hat{f}(\mathbf{h})|^2. \tag{7}$$

The latter variance expression suggests discrepancy measures of the form

$$D(P_n) = \sum_{\mathbf{0}\neq\mathbf{h}\in L_s^*} w(\mathbf{h}) \quad \text{or} \quad D'(P_n) = \sup_{\mathbf{0}\neq\mathbf{h}\in L_s^*} w(\mathbf{h}) \tag{8}$$

where the weights $w(\mathbf{h})$ decrease with the "size" of $\mathbf{h}$ according to how we anticipate $|\hat{f}(\mathbf{h})|^2$ to decrease. In practice, these weights are chosen in heuristic and arbitrary ways. The *spectral test*, which uses the figure of merit $\max_{\mathbf{0}\neq\mathbf{h}\in L_s^*}(1/\|\mathbf{h}\|_2)$, is one example. Other examples include $\mathcal{P}_\alpha$ and $\tilde{\mathcal{P}}_\alpha$; see [7, 8, 20, 31].

## 3 Polynomial Lattice Rules

### 3.1 Definition and basic properties

For an arbitrary integer $b \geq 2$, recall that $\mathbb{Z}_b[z]$ is the ring of polynomials with coefficients in $\mathbb{Z}_b$ and $\mathbb{L}_b$ is the ring of formal Laurent (or power) series with coefficients in $\mathbb{Z}_b$. The *degree* of a series $v(z) = \sum_{\ell=\omega}^{\infty} x_\ell z^{-\ell}$ with $x_\omega \neq 0$ is $\deg(v(z)) = -\omega$. We define $\deg(0) = -\infty$ by convention. The degree of a vector $\mathbf{v}(z) = (v_1(z), \ldots, v_d(z)) \in (\mathbb{L}_b)^d$ is $\max_{1\leq j\leq d} \deg(v_j(z))$. For each integer $\nu$, let

$$\mathbb{L}_{b,\nu} = \mathbb{L}_b \bmod z^{-\nu}\mathbb{Z}_b[z],$$

the set of formal series of degree less than $\nu$, i.e., of the form $\sum_{\ell=\nu+1}^{\infty} x_\ell z^{-\ell}$.

Define the mapping $\varphi : \mathbb{L}_b \to \mathbb{R}$ by

$$\varphi\left(\sum_{\ell=\omega}^{\infty} x_\ell z^{-\ell}\right) = \sum_{\ell=\omega}^{\infty} x_\ell b^{-\ell}.$$

We have $\varphi : \mathbb{L}_b^s \to \mathbb{R}^s$ when $\varphi$ is applied separately to each vector coordinate. Note that $\varphi$ maps $\mathbb{L}_{b,\nu}$ to the hypercube $[0,\, b^{-\nu})^s$.

A *polynomial integration lattice* [18, 21] is a set of the form

$$\mathcal{L}_s = \left\{ \mathbf{v}(z) = \sum_{j=1}^{s} h_j(z)\mathbf{v}_j(z) \text{ such that each } h_j(z) \in \mathbb{Z}_b[z] \right\}, \qquad (9)$$

where $\mathbf{v}_1(z), \ldots, \mathbf{v}_s(z) \in \mathbb{L}_b^s$ are linearly independent over $\mathbb{L}_b$ and $(\mathbb{Z}_b[z])^s \subseteq \mathcal{L}_s$. This set is a module over the ring $\mathbb{Z}_b[z]$. The corresponding *polynomial lattice rule* (PLR) uses the node set $P_n = \varphi(\mathcal{L}_s) \cap [0,1)^s = \varphi(\mathcal{L}_s \cap \mathbb{L}_{b,0})$.

The *key* condition $(\mathbb{Z}_b[z])^s \subseteq \mathcal{L}_s$ implies that each unit vector $\mathbf{e}_j$ can be written as a linear combination of the basis vectors $\mathbf{v}_1(z), \ldots, \mathbf{v}_s(z)$, with coefficients in $\mathbb{Z}_b[z]$. This means that the matrix $\mathbf{V}$ whose rows are these basis vectors has an inverse $\mathbf{V}^{-1}$ whose entries are all in $\mathbb{Z}_b[z]$. Conversely, if all entries of $\mathbf{V}^{-1}$ are in $\mathbb{Z}_b[z]$ and $\mathbf{V}^{-1}$ has an inverse $\mathbf{V}$ with entries in $\mathbb{L}_b$, observing that $\mathbf{V}\mathbf{V}^{-1} = I$, it follows that each $\mathbf{e}_j$ is a linear combination of $\mathbf{v}_1(z), \ldots, \mathbf{v}_s(z)$ with coefficients in $\mathbb{Z}_b[z]$ and thus that $(\mathbb{Z}_b[z])^s \subseteq \mathcal{L}_s$.

The columns of $\mathbf{V}^{-1}$, $\mathbf{h}_1(z)^T, \ldots, \mathbf{h}_s(z)^T$, form a basis of the *dual lattice*

$$\mathcal{L}_s^* = \{\mathbf{h}(z) \in \mathbb{L}_b^s : \mathbf{h}(z) \cdot \mathbf{v}(z) \in \mathbb{Z}_b[z] \text{ for all } \mathbf{v}(z) \in \mathcal{L}_s\},$$

where $\mathbf{h}(z) \cdot \mathbf{v}(z) = \sum_{j=1}^{s} h_j(z)v_j(z)$. One can show that the *determinants* $\det(\mathcal{L}_s) = \det(\mathbf{V})$ and $\det(\mathcal{L}_s^*) = \det(\mathbf{V}^{-1}) = 1/\det(\mathcal{L}_s)$ do not depend on the choice of basis (see [24], Lemma 2). Since the entries of $\mathbf{V}^{-1}$ are in $\mathbb{Z}_b[z]$, $\det(\mathcal{L}_s^*)$ must be a polynomial, say $P(z) = \sum_{l=0}^{k} a_l z^{k-l}$. This polynomial has the multiplicative inverse $1/P(z) = \det(\mathbf{V})$ in the ring $\mathbb{L}_b$, because $\det(\mathbf{V})P(z) = \det(\mathbf{V}\mathbf{V}^{-1}) = 1$, and all entries of $\mathbf{V}$ must be polynomial multiples of $1/P(z)$. Moreover, since $\mathbf{e}_j \in \mathcal{L}_s$ for each $j$, one can always construct a basis $\mathbf{V}$ whose entries have the form $v(z) = 1$ or $v(z) = p(z)/P(z)$ for $p(z) \in \mathbb{Z}_b[z]/(P)$, where $\mathbb{Z}_b[z]/(P)$ denotes the subring of $\mathbb{Z}_b[z]$ in which all operations are performed modulo $P(z)$.

Note that without the condition $(\mathbb{Z}_b(z))^s \subset \mathcal{L}_s$, $\det(\mathbf{V})$ would not necessarily have an inverse in $\mathbb{L}_b$. This condition is crucial for allowing an arbitrary ring $\mathbb{Z}_b$, where $b$ is not necessarily prime.

Each coordinate of $\mathbf{v}(z) \in \mathcal{L}_s$ has the form $v(z) = p(z)/P(z) = \sum_{\ell=w}^{\infty} x_\ell z^{-\ell}$ for some $w$, where $a_0 x_j + a_1 x_{j-1} + \cdots + a_k x_{j-k} = 0$ in $\mathbb{Z}_b$. Any $k+1$ successive digits of a coordinate of any point of $P_n$ also obey this relationship. The polynomial $P(z)$ is a characteristic polynomial of this recurrence. However, it is not necessarily the *minimal* polynomial. Assuming that $p(z) = \sum_{j=1}^{k} c_j z^{k-j}$, we have the following linear bijection between $(c_1, \ldots, c_k)$ and $(x_1, \ldots, x_k)$ [21]:

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ a_1 & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ a_{k-1} & \ldots & a_1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}.$$

For each integer $\nu$, let $\mathcal{L}_{s,\nu} = \mathcal{L}_s \cap \mathbb{L}_{b,\nu}$, the set of lattice points with degree less than $\nu$, and let $s_\nu$ be the dimension of $\mathcal{L}_{s,\nu}$ over $\mathbb{L}_b$. For each $j$, let $-d_j$ be the minimal $\nu$ for which $s_\nu < j$, i.e., for which there are at least $j$ linearly independent points of degree $\leq d_j$, but less than $j$ of degree $< d_j$.

Consider a set of vectors $\tilde{\mathbf{v}}_1(z), \ldots, \tilde{\mathbf{v}}_s(z)$ in $\mathcal{L}_s$ such that for each $\nu < -d_1$, $\tilde{\mathbf{v}}_1(z), \ldots, \tilde{\mathbf{v}}_{s_\nu}(z)$ are $s_\nu$ linearly independent vectors in $\mathcal{L}_{s,\nu}$. This set has the property that $\tilde{\mathbf{v}}_1(z)$ is a nonzero vector of smallest degree in $\mathcal{L}_s$ and, for all $j > 1$, $\tilde{\mathbf{v}}_j(z)$ is a nonzero vector of smallest degree in $\mathcal{L}_s$ independent of $\tilde{\mathbf{v}}_1(z), \ldots, \tilde{\mathbf{v}}_{j-1}(z)$. The fact that $\mathcal{L}_s$ contains $(\mathbb{Z}_b[z])^s$ implies that $\mathcal{L}_{s,1}$ has $s$ dimensions, so $d_1 \leq d_2 \leq \cdots \leq d_s \leq 0$. The numbers $\sigma_j = b^{d_j}$ are called the *successive minima* of $\mathcal{L}_s$. If this set of vectors forms a basis of $\mathcal{L}_s$, then it is a *reduced basis* in the sense of Minkowski.

**Theorem 1.** *(Mahler [23, 24].) If $b$ is a prime (so $\mathbb{Z}_b$ is a field), any set of $s$ vectors with the property described in the previous paragraph is a reduced basis of $\mathcal{L}_s$ over $\mathbb{Z}_b[z]$. Moreover, one has $d_1 + \cdots + d_s = -k$.*

There are similar systems of reduced vectors in the dual lattice $\mathcal{L}_s^*$, with successive minima $\sigma_j^*$ and with $d_j^* = \log_b \sigma_j^*$. In particular, $d_1^*$ is the smallest degree of a nonzero vector in the dual lattice. For prime $b$, Mahler's results also say that these reduced vectors form a basis of the dual lattice and that $\sigma_j^* = 1/\sigma_{s-j+1}$, so $d_j^* = \log_b \sigma_j^* = -d_{s-j+1}$, for $1 \leq j \leq s$.

**Proposition 1.** *For prime $b$, a PLR has* order $n = b^k$ *(i.e., $P_n$ has $b^k$ distinct points) where $k$ is the degree of $P(z)$. We also have $n = b^k$ for general $b$ if we* assume *that $P(z)\mathcal{L}_s$ has a lower-triangular basis whose diagonal elements are all polynomials whose leading coefficients are invertible in $\mathbb{Z}_b$.*

*Proof.* For prime $b$, we use Mahler's reduction theory. Let $\mathbf{v}_1(z), \ldots, \mathbf{v}_s(z)$ be a reduced basis of $\mathcal{L}_s$, where $\mathbf{v}_j$ has degree $d_j \leq 0$ for each $j$, and $d_1 + \cdots + d_s = -k$. By the same argument as in the proof of Theorem 2 of [3], one can show that $\mathcal{L}_s \cap \mathbb{L}_{b,0}$ can be written as the set of all vectors $\mathbf{v}(z) = \sum_{j=1}^s h_j(z)\mathbf{v}_j(z)$ such that $h_j(z)$ is a polynomial of degree less than $-d_j$ in $\mathbb{Z}_b[z]$. This set has cardinality $b^k$ and its elements are all distinct because of the independence of the $\mathbf{v}_j(z)$'s.

For general $b$, under the given assumption, it is possible to adapt the proofs of Lemmas A.4 and A.5 of [21] (given there for $b = 2$). □

The previous proposition covers most cases of practical interest and the result may also hold more generally than under the conditions specified in the proposition. In the remainder of this paper, we shall *assume* that $n = b^k$.

The *rank* of $\mathcal{L}_s$ is the smallest $r$ such that one can find a basis of the form $\mathbf{v}_1(z), \ldots, \mathbf{v}_r(z), \mathbf{e}_{r+1}, \cdots, \mathbf{e}_s$. For a PLR of *rank 1*, one has $\mathbf{v}_1(z) = \mathbf{g}(z)/P(z)$ where $\mathbf{g}(z) = (g_1(z), \ldots, g_s(z)) \in (\mathbb{Z}_b[z]/(P))^s$, $\mathbf{v}_2(z) = \mathbf{e}_2$, …, $\mathbf{v}_s(z) = \mathbf{e}_s$. PLRs of rank 1 were introduced by Niederreiter [25, 26] (see also [27, Section 4.4]). Their generalization to PLRs of arbitrary rank over a finite field was

done in [18, 21]. Here, for Proposition 1 to apply, it suffices that the leading coefficient of $g_1(z)$ has no common factor with $b$.

If $\mathbf{g}(z) = (1,\ a(z),\ a^2(z) \bmod P(z),\ \ldots,\ a^{s-1}(z) \bmod P(z))$ where $P(z)$ is a polynomial of degree $k$ over $\mathbb{Z}_b$, having a multiplicative inverse $1/P(z)$ in $\mathbb{L}_b$, and $a(z) \in \mathbb{Z}_b[z]/(P)$, we have a *Korobov* PLR. The latter is equivalent to using the point set

$$P_n = \{\varphi((p_0(z), \ldots, p_{s-1}(z))/P(z)) \ :\ p_0(z) \in \mathbb{Z}_b[z]/(P)\}$$

where $p_j(z) = a(z)p_{j-1}(z) \bmod P(z)$ for all $j$. This is the image by $\varphi$ of the set of all vectors of successive values produced by an LCG defined in a space of polynomials, with modulus $P(z)$ and multiplier $a(z)$, from all initial states $p_0(z)$. Again, if the polynomial LCG has maximal period length, this may provide an efficient way of enumerating $P_n$.

As a special case, let $b = 2$ and $a(z) = z^\nu \bmod P(z)$ for some integer $\nu > 0$. Then, $p_i(z)/P(z) = z^\nu p_{i-1}(z)/P(z) \bmod \mathbb{Z}_2[z]$, so to obtain the coefficients of the power series $p_i(z)/P(z)$ it suffices to shift the coefficients of $p_{i-1}(z)/P(z)$ by $\nu$ positions and to drop the nonnegative powers of $z$. This corresponds to using all cycles of a *linear feedback shift register* (LFSR) generator with characteristic polynomial $P(z)$ and *step size* $\nu$ [21, 32, 35, 34].

The projection of $\mathcal{L}_s$ over the subspace determined by $I = \{i_1, \ldots, i_\eta\} \subset \{1, \ldots, s\}$ is a polynomial integration lattice $\mathcal{L}_s(I)$ with dual lattice $\mathcal{L}_s^*(I)$ and point set $P_n(I)$. The following is proved in [21] for $b = 2$ and the proof can be adapted to arbitrary $b$ under the additional condition that none of the $g_j(z)$ is a divisor of zero.

**Proposition 2.** *A rule of rank 1 with* $\mathbf{v}_1(z) = (g_1(z), g_2(z), \ldots, g_s(z))/P(z)$ *is fully projection-regular iff for all* $j$, $\gcd(g_j(z), P(z)) = 1$ *and there is no polynomial* $u_j(z) \neq 0$ *such that* $u_j(z)g_j(z) = 0$. *A Korobov rule, with* $g_j(z) = a^{j-1}(z) \bmod P(z)$, *is fully projection-regular and dimension-stationary iff* $\gcd(a(z), P(z)) = 1$ *and there is no polynomial* $u(z) \neq 0$ *such that* $u(z)a(z) = 0$.

### 3.2 Link with ordinary lattice rules

Consider an ordinary lattice rule $L_s$ of rank 1 with $n$ points and first basis vector $\mathbf{v}_1 = (a_1, \ldots, a_s)/n$ such that $\gcd(a_1, n) = 1$, $a_j < n$ for all $j$, and $\mathbf{v}_j = \mathbf{e}_j$ for $j > 1$. Then, $a_1$ has a multiplicative inverse in $\mathbb{Z}_n$, say $a_1^*$. Let $b = n$. Define the polynomial lattice $\mathcal{L}_s$ of rank 1 with basis $\mathbf{v}_1(z) = (g_1(z), \ldots, g_s(z))/P(z) = (a_1, \ldots, a_s)z^{-1}$ where $P(z) = z$ and $\mathbf{v}_j(z) = \mathbf{e}_j$ for $j > 1$. One has $\mathbf{e}_1 = a_1^*[\mathbf{v}_1(z)P(z) - a_2\mathbf{v}_2(z) - \cdots - a_s\mathbf{v}_s(z)]$, so $\mathcal{L}_s$ is an integration lattice. One can verify that the two rules $L_s$ and $\mathcal{L}_s$ have exactly the same point set $P_n$. This shows that some ordinary lattice rules can be expressed as polynomial lattice rules.

### 3.3 Sums of polynomial lattices

Given $m$ polynomial lattices $\mathcal{L}_s^1, \ldots, \mathcal{L}_s^m$, let $\mathcal{L}_s = \mathcal{L}_s^1 + \cdots + \mathcal{L}_s^m = \{\mathbf{w}_1(z) + \cdots + \mathbf{w}_s(z) : \mathbf{w}_j(z) \in \mathcal{L}_s^j \text{ for each } j\}$. In terms of point sets, $\mathcal{L}_s$ corresponds to the *sum rule* with $P_n = P_{n_1} + \ldots + P_{n_m}$, where $P_{n_j}$ comes from $\mathcal{L}_s^j$ and "+" denotes the digitwise addition in $\mathbb{Z}_b$. If $b = 2$, this means bitwise exclusive-or. In general, sum rules are useful because they can make it easier to obtain high quality rules (in terms of measures of uniformity) having efficient implementations. The idea is to define the rule in a way that each $P_{n_j}$ is easy to enumerate (but may have poor quality if used alone) and the sum $P_n$ has good quality (but may be inefficient to enumerate without using the decomposition). The proof of the following proposition is left as an exercise.

**Proposition 3.** *For prime $b$, if the $ms$ basis vectors of $\mathcal{L}_s^1, \ldots, \mathcal{L}_s^m$ are independent over $\mathbb{Z}_b[z]$ and $n_j = b^{k_j}$, then $P(z) = 1/\det(\mathcal{L}_s)$ has degree $k$ and the sum rule has $n = b^k$ points, where $k = k_1 + \cdots + k_m$. This holds in particular if the polynomials $P_j(z) = 1/\det(\mathcal{L}_s^j)$ are pairwise relatively prime. Moreover, if $\mathcal{L}_s^j$ has rank $r_j$ for each $j$, then $\mathcal{L}_s$ has rank $r = \max(r_1, \ldots, r_m)$.*

*Example 1. Combined LFSR generators.* Take $m$ LFSR generators with pairwise relatively prime characteristic polynomials $P_j(z)$ of degree $k_j$ and step size $\nu_j$, for $j = 1, \ldots, m$, and combine their outputs via a bitwise xor. This provides an efficient way of implementing a LFSR generator whose characteristic polynomial $P(z) = P_1(z) \cdots P_m(z)$ has many nonzero coefficients, by taking components whose polynomials $P_j(z)$ have very few nonzero coefficients and which can be implemented efficiently [16, 35].

*Example 2. Rectangular rule.* Choose $d$ in $\{1, \ldots, s\}$, and let $\mathbf{v}_j(z) = \mathbf{e}_j/Q(z)$ for $j \le d$ and $\mathbf{v}_j(z) = \mathbf{e}_j$ for $j > d$, where $Q(z)$ has degree $q$. This rule has rank $d$ with $P(z) = \det(\mathcal{L}_s^*) = (Q(z))^d$, and order $n = b^k = b^{qd}$. It is a sum rule with $\mathcal{L}_s^j$ the rank-1 lattice generated by $\mathbf{v}_j(z)$ and the unit vectors, whose $2^q$ points are all on axis $j$, evenly spaced, for $1 \le j \le d$. This rule is obviously *not* projection-regular. The corresponding point set is a *rectangular grid* in the first $d$ dimensions.

### 3.4 Extensible rules

As for ordinary lattices, one can define a sequence of imbedded polynomial integration lattices $\mathcal{L}_s^1 \subset \mathcal{L}_s^2 \subset \mathcal{L}_s^3 \subset \ldots$ [21, 28]. Again, if $\varphi(\mathcal{L}_s^\xi) \cap [0,1)^s$ has $n_\xi$ points, then $n_{\xi-1}$ must divide $n_\xi$ for each $\xi$. If $P_{\xi-1}(z)$ divides $P_\xi(z)$ for each $\xi$, where $P_\xi(z) = 1/\det(\mathcal{L}_s^\xi)$, and if each $\mathcal{L}_s^\xi$ has a basis $\mathbf{v}_{1,\xi}(z), \ldots, \mathbf{v}_{s,\xi}(z)$ where $\mathbf{v}_{j,\xi-1}(z) = \mathbf{v}_{j,\xi}(z) \bmod P_{\xi-1}(z)$, then $\mathcal{L}_s^{\xi-1}$ is a sublattice of $\mathcal{L}_s^\xi$ for each $\xi$.

For example, $\mathcal{L}_\xi$ can be a Korobov polynomial lattice (i.e., based on a polynomial LCG) with modulus $P_\xi(z)$ and multiplier $a_\xi(z)$, where $P_{\xi-1}(z)$ divides $P_\xi(z)$ and $a_{\xi-1}(z) = a_\xi(z) \bmod P_{\xi-1}(z)$, for each $\xi$. A simple choice is $P_\xi(z) = z^\xi$, so $n_\xi = b^\xi$, and $a_\xi(z) = a_{\xi-1}(z) + \nu_\xi z^{\xi-1}$ for some $\nu_\xi \in \mathbb{Z}_b$, for each $\xi$.

### 3.5 Random digital shift, Walsh expansion, and variance expressions

To shift randomly a polynomial lattice, a random vector is generated uniformly in $\mathbb{L}_{b,0}^s$ and added to each vector of $\mathcal{L}_s$, modulo $(\mathbb{Z}_b[z])^s$. This is equivalent to generating a random vector $\mathbf{U}$ uniformly in $[0,1)^s$ and adding its digital $b$-ary expansion to that of each point of $P_n$, digit by digit, in $\mathbb{Z}_b$. The latter is actually defined for *any* type of point set $P_n$ and it is called a *digital random shift*. Just as with ordinary random shifts, to obtain an unbiased estimator of $\mu$ together with a variance estimate (or confidence interval) from an arbitrary $P_n$, one can make $m$ independent digital random shifts of $P_n$. If $\bar{X}$ and $S_x^2$ are the sample mean and variance of the $m$ corresponding values of $Q_n$ (after the shifts), then $\mathrm{E}[\bar{X}] = \mu$ and $\mathrm{E}[S_x^2] = \mathrm{Var}[Q_n] = m\mathrm{Var}[\bar{X}]$, regardless of the type of point set $P_n$.

Variance expressions for PLRs with digital random shifts can be obtained via Walsh expansions, defined as follows. For $\mathbf{h} \equiv \mathbf{h}(z) = (h_1(z), \ldots, h_s(z)) \in (\mathbb{Z}_b[z])^s$ and $\mathbf{u} = (u_1, \ldots, u_s) \in [0,1)^s$, where

$$h_j(z) = \sum_{i=0}^{\ell_j - 1} h_{j,i} z^i, \qquad u_j = \sum_{\ell \geq 1} u_{j,\ell} b^{-\ell} \in [0,1),$$

and $u_{j,\ell} \neq b-1$ for infinitely many $\ell$, define

$$\langle \mathbf{h}, \mathbf{u} \rangle = \sum_{j=1}^{s} \sum_{\ell=0}^{\ell_j - 1} h_{j,\ell} u_{j,\ell+1} \quad \text{in } \mathbb{Z}_b.$$

The *Walsh expansion* in base $b$ of $f : [0,1)^s \to \mathbb{R}$ is

$$f(\mathbf{u}) = \sum_{\mathbf{h} \in (\mathbb{Z}_b[z])^s} \tilde{f}(\mathbf{h}) e^{2\pi\sqrt{-1}\langle \mathbf{h}, \mathbf{u} \rangle / b},$$

with Walsh coefficients

$$\tilde{f}(\mathbf{h}) = \int_{[0,1)^s} f(\mathbf{u}) e^{-2\pi\sqrt{-1}\langle \mathbf{h}, \mathbf{u} \rangle / b} d\mathbf{u}.$$

The following propositions are proved in [21] for $b = 2$ and can be extended to an arbitrary $b \geq 2$.

**Proposition 4.** *If $P_n = \{\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}\}$ is the point set of a polynomial lattice $\mathcal{L}_s$, then*

$$\frac{1}{n} \sum_{i=0}^{n-1} e^{2\pi\sqrt{-1}\langle \mathbf{h}, \mathbf{u}_i \rangle / b} = \begin{cases} 1 \text{ if } \mathbf{h} \in \mathcal{L}_s^*, \\ 0 \text{ otherwise.} \end{cases}$$

*Moreover, if the Walsh series expansion of $f$ converges absolutely, then*

$$E_n = \sum_{\mathbf{0} \neq \mathbf{h} \in \mathcal{L}_s^*} \tilde{f}(\mathbf{h}).$$

**Proposition 5.** *Suppose* $\sigma^2 < \infty$. *Then,*

$$\sigma^2 = \sum_{\mathbf{0}\neq\mathbf{h}\in(\mathbb{Z}_b[z])^s} |\tilde{f}(\mathbf{h})|^2.$$

*If* $P_n$ *is the digital random shift of a PLR* $\mathcal{L}_s$, *then*

$$\mathrm{Var}[Q_n] = \sum_{\mathbf{0}\neq\mathbf{h}\in\mathcal{L}_s^*} |\tilde{f}(\mathbf{h})|^2.$$

Again, this last variance expression suggests discrepancy measures for PLRs of the form

$$D(P_n) = \sum_{\mathbf{0}\neq\mathbf{h}\in\mathcal{L}_s^*} w(\mathbf{h}) \quad \text{or} \quad D'(P_n) = \sup_{\mathbf{0}\neq\mathbf{h}\in\mathcal{L}_s^*} w(\mathbf{h}) \tag{10}$$

where the weights $w(\mathbf{h})$ decrease with the "size" of $\mathbf{h}$ according to how we expect $|\tilde{f}(\mathbf{h})|^2$ to decrease. Specific choices of $w$ will be mentioned in section 3.8.

### 3.6 Equidistribution and $(t, k, s)$-net property

For an arbitrary vector of non-negative integers $\mathbf{q} = (q_1, \ldots, q_s)$, partition $[0,1)^s$ along the $j$th axis into $b^{q_j}$ equal subintervals, for each $j$. This gives $b^{q_1+\cdots+q_s}$ rectangular boxes of the same size and shape. We call this partition the $\mathbf{q}$-*equidissection* of the unit hypercube.

For $n = b^k$, $P_n$ is called $\mathbf{q}$-*equidistributed in base* $b$ if it has $b^t$ points in each box, where $t = k - q_1 - \cdots - q_s$. Of course, this can hold only if $t \geq 0$. If this holds for $q_1 = \cdots = q_s = \ell$ for some integer $\ell \geq 1$, we have $s$-*distribution with* $\ell$ *digits of accuracy* [6, 15]. The largest such $\ell$ is the $s$-*dimensional resolution* of $P_n$. It cannot exceed $\lfloor k/s \rfloor$.

This notion of equidistribution can also be defined for projections. For $I = \{i_1, \ldots, i_\eta\} \subset \{1, \ldots, s\}$, divide each axis $i_j$ into $b^{q_{i_j}}$ intervals to obtain $b^{k-t(I)}$ rectangular boxes, where $k - t(I) = q_{i_1} + \ldots + q_{i_\eta}$. The set $P_n(I)$ is called $(q_{i_1}, \ldots, q_{i_\eta})$-*equidistributed* if each box contains $2^{t(I)}$ points.

A point set $P_n$ with $n = b^k$ is called a $(t, k, s)$-*net in base* $b$ if it is $(q_1, \ldots, q_s)$-equidistributed for all non-negative integers $q_1, \ldots, q_s$ summing to $k - t$. We call the smallest such $t$ the $t$-*value* of the net.

### 3.7 Measuring uniformity via the shortest nonzero vector or a reduced basis of $\mathcal{L}_s^*$.

The equidistribution and $(t, k, s)$-net properties can be verified by computing the length of a shortest nonzero vector in $\mathcal{L}_s^*$, as we now explain.

Suppose we are interested in the $\mathbf{q}$-equidistribution for a polynomial integration lattice $\mathcal{L}_s$ and a fixed $\mathbf{q} = (q_1, \ldots, q_s) \geq \mathbf{0}$. For a given vector

$\mathbf{v}(z) \in \mathcal{L}_{s,0}$, all powers of $z$ less than $-q_j$ in coordinate $j$ of $\mathbf{v}(z)$ are irrelevant for determining in which box of this $\mathbf{q}$-equidissection $\varphi(\mathbf{v}(z))$ falls, so we can truncate them. In other words, we define a mapping $\mathrm{trunc}_{\mathbf{q}} : \mathcal{L}_s \to \mathcal{L}_s$ that transforms the $j$th coordinate $v_j(z) = \sum_{\ell=w}^{\infty} x^\ell z^{-\ell}$ into

$$\mathrm{trunc}_{\mathbf{q}}(v_j(z)) = \sum_{\ell=w}^{q_j} x^\ell z^{-\ell}.$$

This mapping is linear over $\mathbb{Z}_b$ and its kernel is the set of points mapped by $\varphi$ to the box that contains the origin, $B_0 = \prod_{j=1}^{s} [0, b^{-q_j})$. If $d$ is the dimension of this kernel over $\mathbb{Z}_b$, then there are $b^d$ points that are mapped to this box and each point in the image of $\mathrm{trunc}_{\mathbf{q}}$ also has $b^d$ pre-images. This means that each of the $b^{k-t}$ boxes of the $\mathbf{q}$-equidissection contains either no point or $b^d$ points. The total number of points being $b^k$, it follows that there are $b^{k-d}$ boxes with $b^d$ points each, and the fraction of boxes that are occupied is $b^{t-d}$. Note that $t = k - q_1 - \cdots - q_s$ can be negative. An important issue is to figure out how to compute $d$. This was done in [3] for the special case where $b = 2$ and all the $q_j$ are equal.

To treat the more general case, we will rescale the integration lattice $\mathcal{L}_s$ linearly in a way that the box $B_0$ becomes the unit hypercube. We define the $\mathbf{q}$-*inflated lattice* $\mathcal{L}_s^{\uparrow\mathbf{q}}$ by

$$\mathcal{L}_s^{\uparrow\mathbf{q}} = \{\tilde{\mathbf{v}}(z) = (z^{q_1} v_1(z), \ldots, z^{q_s} v_s(z)) : \mathbf{v}(z) = (v_1(z), \ldots, v_s(z)) \in \mathcal{L}_s\}.$$

Its dual is the $\mathbf{q}$-*deflated* dual lattice

$$\mathcal{L}_s^{*\downarrow\mathbf{q}} = \left\{\tilde{\mathbf{h}}(z) = (z^{-q_1} h_1(z), \ldots, z^{-q_s} h_s(z)) : \mathbf{h}(z) = (h_1(z), \ldots, h_s(z)) \in \mathcal{L}_s^*\right\}.$$

Note that $\mathcal{L}_s^{\uparrow\mathbf{q}}$ is not necessarily an integration lattice, but $\det(\mathcal{L}_s^{*\downarrow\mathbf{q}}) = z^{-q_1-\cdots-q_s} \det(\mathcal{L}_s^*) = z^{t-k} P(z) \stackrel{\text{def}}{=} \tilde{P}(z)$ has a multiplicative inverse if $P(z)$ has one and $\det(\mathcal{L}_s^{\uparrow\mathbf{q}}) = 1/\tilde{P}(z) = z^{k-t}/P(z)$. Now, $b^d$ is the cardinality of the set $[0,1)^s \cap \varphi(\mathcal{L}_s^{\uparrow\mathbf{q}})$.

For case where $b$ is prime, we can use Mahler's theory and the results of [3] to determine $d$. (These results were proved only for $b = 2$, but their generalization to an arbitrary prime $b$ is easy.) So for prime $b$, Theorem 1 tells us that the lattice $\mathcal{L}_s^{\uparrow\mathbf{q}}$ has a reduced basis in which the $j$th vector has degree $d_j = \log_b \sigma_j$, where $\sigma_1, \ldots, \sigma_s$ are the successive minima. These numbers satisfy $d_1 + \cdots + d_s = -\deg(\tilde{P}(z)) = -k + q_1 + \cdots + q_s = -t$. There is also a similar reduced basis in the dual lattice $\mathcal{L}_s^{*\downarrow\mathbf{q}}$, with successive minima $\sigma_j^*$ that satisfy $\sigma_j^* = 1/\sigma_{s-j+1}$, so $d_j^* = \log_b \sigma_j^* = -d_{s-j+1}$, for $1 \le j \le s$.

Theorem 2 of [3], generalized to an arbitrary prime $b > 2$ and applied to $\mathcal{L}_s^{\uparrow\mathbf{q}}$, tells us that

$$d = \sum_{j=1}^{s} \max(0,\, -d_j) = \sum_{j=1}^{s} \max(0,\, d_j^*). \tag{11}$$

In particular, all boxes contain the same number of points iff $d = t = d_1^* + \cdots + d_s^*$, iff $d_j^* \geq 0$ for all $j$, iff $d_1^* \geq 0$, iff $\sigma_1^* \geq 1$. We have just proved the following:

**Proposition 6.** *Let $b$ be prime. In the $\mathbf{q}$-equidissection of $[0,1)^s$, there are exactly $b^{k-d}$ boxes with $b^d$ points from $P_n$ each, and all other boxes are empty, where $d$ is given by (11). Moreover, $P_n$ is $\mathbf{q}$-equidistributed iff $\sigma_1^* \geq 1$.*

The *$s$-dimensional resolution* of $P_n$ is the largest integer $\ell$ such that $P_n$ is $\mathbf{q}$-equidistributed for $\mathbf{q} = (\ell, \ldots, \ell)$, i.e., the largest $\ell$ such that $d_1^* \geq 0$ for this $\mathbf{q}$. But observe that $d_1^* \geq 0$ in $\mathcal{L}_s^{*\downarrow\mathbf{q}}$ for $\mathbf{q} = (\ell, \ldots, \ell)$ iff $d_1^* \geq \ell$ in $\mathcal{L}_s^{*\downarrow\mathbf{q}} = \mathcal{L}_s^*$ for $\mathbf{q} = (0, \ldots, 0)$. This gives:

**Proposition 7.** *Let $b$ be prime. The resolution of $P_n$ is equal to the value of $d_1^*$ that corresponds to $\mathbf{q} = (0, \ldots, 0)$.*

If we define the distance function $\|\cdot\|_{\mathbf{0}}$ on $\mathcal{L}_s^{\uparrow\mathbf{q}}$ and $\mathcal{L}_s^{*\downarrow\mathbf{q}}$ by

$$\log_b \|\mathbf{v}(z)\|_{\mathbf{0}} = \deg(\mathbf{v}(z)), \tag{12}$$

then $\sigma_1^*$ can be interpreted as the length of the shortest nonzero vector in the dual lattice $\mathcal{L}_s^{*\downarrow\mathbf{q}}$:

$$\sigma_1^* = \min_{\mathbf{0} \neq \mathbf{h}(z) \in \mathcal{L}_s^{*\downarrow\mathbf{q}}} \|\mathbf{h}(z)\|_{\mathbf{0}},$$

and $\sigma_j^*$ as the length of the $j$th vector in a reduced basis of $\mathcal{L}_s^{*\downarrow\mathbf{q}}$.

Working with the distance function $\|\cdot\|_{\mathbf{0}}$ and with the lattices $\mathcal{L}_s^{\uparrow\mathbf{q}}$ and $\mathcal{L}_s^{*\downarrow\mathbf{q}}$ is actually equivalent to working in the original lattices but using the distances $\|\cdot\|_{\mathbf{q}}$ on $\mathcal{L}_s$ and $\|\cdot\|_{-\mathbf{q}}$ on $\mathcal{L}_s^*$, where

$$\log_b \|\mathbf{v}(z)\|_{\mathbf{q}} = \max_{1 \leq j \leq s} (\deg(v_j(z)) + q_j) = \deg((z^{q_1} v_1(z), \ldots, z^{q_s} v_s(z)). \tag{13}$$

The successive minima with respect to these distances in the original lattice and its dual are exactly the same as the successive minima $\sigma_1, \ldots, \sigma_s$ and $\sigma_1^*, \ldots, \sigma_s^*$ defined earlier. Propositions 6 and 7 could therefore be restated in terms of the successive minima in the original dual lattice with the distance $\|\cdot\|_{-\mathbf{q}}$.

By changing the definition of vector length, the $t$-value of $P_n$ can also be obtained by computing the length of a shortest nonzero vector in the dual lattice. For $\mathbf{h} = \mathbf{h}(z) \in \mathbb{Z}_b[z]$, define $\|\mathbf{h}\|_\pi$ by

$$\log_b \|\mathbf{h}\|_\pi = \sum_{j=1}^{s} \deg(h_j)$$

and let $\tau_1^* = \min_{\mathbf{0} \neq \mathbf{h} \in \mathcal{L}_s^*} \|\mathbf{h}\|_\pi$. The following result is a consequence of Proposition 16 (ii) of section 5.2.

**Proposition 8.** *The $t$-value of $P_n$ is equal to $k - s + 1 - \log_b \tau_1^*$.*

Standard algorithms can be used for computing the shortest vector or the successive minima in a polynomial lattice when $b$ is prime (see, e.g., [22, 34]). The efficiency of such algorithms depends on the definition of vector length and this is a major factor to consider when selecting a "practical" figure of merit. In particular, the length of the shortest vector is much easier to compute for the distance function $\|\cdot\|_{\mathbf{0}}$ defined in (12) than for $\|\cdot\|_{\pi}$. This gives motivation for using the former.

### 3.8 Selection criteria

There are many ways of defining selection criteria for highly uniform point sets, including polynomial lattice rules and digital nets [18, 20, 27]. The following class of criteria, based on equidistribution in "cubic" equidissections, were proposed in [20, 21]. For an arbitrary set of indices $I = \{i_1, i_2, \ldots, i_\eta\}$, we define the *resolution gap* of $P_n(I)$ as $\delta_I = \lfloor k/d \rfloor - \ell_I$, where $\ell_I$ is the $\eta$-dimensional *resolution* of $P_n(I)$. A worst-case figure of merit can be defined as $\Delta_{\mathcal{J}} = \max_{I\in\mathcal{J}} \delta_I$ where $\mathcal{J}$ is a selected class of sets $I$. The choice of $\mathcal{J}$ is a question of compromise. If $\mathcal{J}$ contains too many sets, not only the selection criterion will be more costly to compute, but the best value of $\Delta_{\mathcal{J}}$ that can be achieved will be larger, and therefore the criterion will become less demanding for the equidistribution of the low-dimensional projections that could be considered more important.

Assuming that $P_n$ is dimension-stationary, Lemieux and L'Ecuyer [20] suggest selecting some positive integers $\eta, s_1, \ldots, s_\eta$, and taking

$$\begin{aligned}\mathcal{J} = &\{\{0, 1, \ldots, i\} : i < s_1\} \\ &\cup \{\{i_1, i_2\} : 0 = i_1 < i_2 < s_2\} \cup \cdots \\ &\cup \{\{i_1, \ldots, i_\eta\} : 0 = i_1 < \ldots < i_\eta < s_\eta\}.\end{aligned}$$

If we denote by $\Delta_{s_1,\ldots,s_\eta}$ the corresponding $\Delta_{\mathcal{J}}$, $\Delta_k = 0$ means *maximally equidistributed* and a $(t, k, s)$-net always has $\Delta_{k,\ldots,k} \le t$ (but not vice-versa). To break ties, one can use a larger set $\mathcal{J}$ in a second stage, or use $\sigma_{\mathcal{J}} = \sum_{I\in\mathcal{J}} \delta_I$ as a secondary criterion.

*Example 3.* (Provided by F. Panneton) Consider the Korobov PLR with $b = 2$, $k = 15$, $P(z) = z^{15} + z^{12} + z^{11} + z^8 + z^7 + z^4 + z^3 + z + 1$, and $a(z) = z^{53} \bmod P(z)$. This rule is projection-regular and dimension-stationary. It also has $n = 2^{15}$ points and $\Delta_{15,12,5} = 0$.

A criterion based on the $t$-values of projections and that recognizes the importance of low-dimensional projections can be defined as (see [18])

$$\max_{I\in\mathcal{J}} t^*_{|I|}/t_I,$$

where $t_I$ is the $t$-value for $P_n(I)$ and $t^*_{|I|}$ a lower bound on the best possible $t$-value in $|I|$ dimensions, with the convention that $0/0 = 1$. This figure of

merit always lies in $(0, 1]$ and we want it to be large (the optimal value is 1). Another possibility is

$$\max_{I \in \mathcal{J}} (t_I - t^*_{|I|}),$$

whose value is always a non-negative integer and we want it to be small (the optimal value is 0).

For ordinary lattice rules, Hickernell [8] introduced a general figure of merit called $\tilde{\mathcal{P}}_\alpha$ that can give arbitrary weights to the projections. It is justified by error expressions for specific classes of functions. A version of this criterion for the polynomial case, with $\alpha = 2$ and product-type weights, was defined in [18, 21] as follows

$$\tilde{\mathcal{P}}_{2,\mathrm{PLR}} = \sum_{\mathbf{0} \neq \mathbf{h} \in \mathcal{L}^*_s} \beta_0^2 \prod_{\{j : h_j \neq 0\}} \beta_j^2 b^{-2 \deg(h_j)}$$

where $\beta_j > 0$ for $j = 0, \ldots, s$. In the case of a polynomial lattice point set with $b = 2$, this simplifies to an expression that can be computed in $O(ns)$ time.

## 4 Resolutionwise Polynomial Lattice Rules

In dimensionwise (or ordinary) polynomial integration lattices, the coordinates of the $s$-dimensional lattice vectors correspond to point coordinates. In resolutionwise lattices, the lattice vectors are $\ell$ dimensional, each of their coordinates corresponds to one specific digit in the $b$-ary expansion of the points, and the coefficients of $z^{-j}$ in their coordinates determine these digits for the $j$th dimension, for up to $\ell$ digits of resolution.

The motivation for considering such constructions is that they cover several methods that are very popular in the context of random number generation and whose point sets do not fit the definition of dimensionwise PLR given in the previous section. These methods include for instance GFSR and twisted GFSR generators, Tausworthe generators with linear tempering, and many others; see [2, 21, 19, 34].

We define a *resolutionwise polynomial integration lattice* by

$$\mathcal{R}_\ell = \left\{ \mathbf{w}(z) = \sum_{m=1}^{\ell} h_m(z) \mathbf{w}_m(z) \text{ such that each } h_m(z) \in \mathbb{Z}_b[z] \right\},$$

where $\mathbf{w}_1(z), \ldots, \mathbf{w}_\ell(z)$ are in $\mathbb{L}_b^\ell$ and $\mathcal{R}_\ell$ contains $(\mathbb{Z}_b[z])^\ell$. Define $\psi_s : \mathbb{L}_b^\ell \to [0, 1)^s$ as follows. For

$$\mathbf{w}(z)^T = \begin{pmatrix} w_1(z) \\ \vdots \\ w_\ell(z) \end{pmatrix} = \begin{pmatrix} \cdots & w_{1,1} & \cdots & w_{1,s} & \cdots \\ & \vdots & & \vdots & \\ \cdots & w_{\ell,1} & \cdots & w_{\ell,s} & \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ z^{-1} \\ \vdots \\ z^{-s} \\ \vdots \end{pmatrix}, \qquad (14)$$

let

$$\psi_s(\mathbf{w}(z)) = \left( \sum_{q=1}^{\ell} w_{q,1} b^{-q},\ \cdots,\ \sum_{q=1}^{\ell} w_{q,s} b^{-q} \right).$$

The corresponding rule uses the point set $P_n = \psi_s(\mathcal{R}_\ell \cap \mathbb{L}_{b,0}^{\ell})$. The basis vectors form a matrix

$$\mathbf{W} = \begin{pmatrix} \mathbf{w}_1(z) \\ \vdots \\ \mathbf{w}_\ell(z) \end{pmatrix}$$

with inverse

$$\mathbf{W}^{-1} = \left( \mathbf{h}_1(z)^T \cdots \mathbf{h}_\ell(z)^T \right),$$

whose columns form a basis of the *dual lattice*

$$\mathcal{R}_\ell^* = \{\mathbf{h}(z) \in \mathbb{L}_b^{\ell} : \mathbf{h}(z) \cdot \mathbf{w}(z) \in \mathbb{Z}_b[z] \text{ for all } \mathbf{w}(z) \in \mathcal{R}_\ell\}.$$

As for dimensionwise PLRs, $(\mathbb{Z}_b[z])^\ell \subseteq \mathcal{R}_\ell$ iff all entries of $\mathbf{W}^{-1}$ are polynomials. Then, $\det(\mathcal{R}_\ell^*) = \det(\mathbf{W}^{-1}) = P(z)$, a polynomial of degree $k \le s\ell$, and all entries of $\mathbf{W}$ are polynomial multiples of $1/P(z)$, so their $b$-ary expansions follow a recurrence with characteristic polynomial $P(z)$. One can always find a basis $\mathbf{W}$ whose entries have the form $w(z) = 1$ or $w(z) = p(z)/P(z)$ where $\deg(p(z)) < k$.

If $b$ is prime, the lattice $\mathcal{R}_\ell$ also has a reduced basis in the sense of Theorem 1. Let us assume that $\mathbf{w}_1(z), \ldots, \mathbf{w}_\ell(z)$ is such a reduced basis, with successive minima $\|\mathbf{w}_m(z)\|_{\mathbf{0}} = b^{d_m}$ for $1 \le m \le \ell$. We have $d_j \le 0$ for all $j$ and $d_1 + \cdots + d_s = -k$. Then, as in the proof of Proposition 1, $\mathcal{R}_\ell \cap \mathbb{L}_{b,0}^{\ell}$ can be written as the set of vectors $\mathbf{w}(z) = \sum_{m=1}^{\ell} h_m(z)\mathbf{w}_m(z)$ such that $h_m(z)$ is a polynomial of degree less than $-d_j$ in $\mathbb{Z}_b[z]$. This set has cardinality $b^k$ and its elements are all distinct, because the $\mathbf{w}_j(z)$'s are independent. We have just proved:

**Proposition 9.** *If $b$ is prime, the set $P_n = \psi_s(\mathcal{R}_\ell \cap \mathbb{L}_{b,0}^{\ell})$ contains $n = b^k$ distinct points.*

If $b$ is not prime, one can also prove that $n = b^k$ under additional conditions on the basis, as in Proposition 1.

### 4.1 A resolutionwise PLR can be reformulated as a digital net

One can see that the point set of a resolutionwise polynomial integration lattice is a special case of a digital net, at least for prime $b$, as follows. Again, we assume that $\mathbf{w}_1(z), \ldots, \mathbf{w}_\ell(z)$ is a reduced basis, with successive minima $\|\mathbf{w}_m(z)\|_{\mathbf{0}} = b^{d_m}$, $1 \le m \le \ell$. Let $\mathbf{u} = \psi_s(\mathbf{w}(z)) = \psi_s\left(\sum_{m=1}^{\ell} h_m(z)\mathbf{w}_m(z)\right) \in P_n$. Its $j$th coordinate can be written as $u_j = \sum_{q=1}^{\ell} w_{q,j} b^{-q}$. If we write

$$\mathbf{w}_m(z) = \left(\sum_{j=1}^{\infty} w_{m,1,j} z^{-j}, \ldots, \sum_{j=1}^{\infty} w_{m,\ell,j} z^{-j}\right) \quad \text{and} \quad h_m(z) = \sum_{p=0}^{-d_m-1} a_{m,p} z^p,$$

expand the equation

$$w_q(z) = \sum_{j=j_q}^{\infty} w_{q,j} z^{-j} = \sum_{m=1}^{\ell} h_m(z) \sum_{j=0}^{\infty} w_{m,q,j} z^{-j},$$

and collect the corresponding powers of $z$, we find that for each coordinate $j$,

$$\begin{pmatrix} w_{1,j} \\ \vdots \\ w_{\ell,j} \end{pmatrix} = \sum_{m=1}^{\ell} \boldsymbol{\Gamma}_m^{(j)} \begin{pmatrix} a_{m,0} \\ \vdots \\ a_{m,-d_m-1} \end{pmatrix},$$

where

$$\boldsymbol{\Gamma}_m^{(j)} = \begin{pmatrix} w_{m,1,j} & w_{m,1,j+1} & \cdots & w_{m,1,j-d_m-1} \\ \vdots & \vdots & & \vdots \\ w_{m,\ell,j} & w_{m,\ell,j+1} & \cdots & w_{m,\ell,j-d_m-1} \end{pmatrix}.$$

So we have a special case of a digital net, with generating matrices $\mathbf{C}^{(j)} = (\boldsymbol{\Gamma}_1^{(j)} \; \boldsymbol{\Gamma}_2^{(j)} \; \cdots \; \boldsymbol{\Gamma}_\ell^{(j)})$ of dimension $\ell \times k$. These generating matrices can be extended to $\infty \times k$ matrices by appending rows of zeros.

Whenever $\mathbf{w}_m(z) \in (\mathbb{Z}_b[z])^\ell$, $\boldsymbol{\Gamma}_m^{(j)} = \mathbf{0}$. In particular, if the rule has rank $r$ and $\mathbf{w}_m = \mathbf{e}_m$ for $m > r$, then $\boldsymbol{\Gamma}_m^{(j)} = \mathbf{0}$ for $m > r$.

### 4.2 Equidistribution

The inflation/deflation trick introduced in section 3.7 does not work here, because the digits $w_{q,j}$ for a given dimension $j$ are taken from different coordinates of $\mathbf{w}(z)$. However, it is still possible to prove the following proposition:

**Proposition 10.** *Assume that $b$ is prime. Let $b^{d_1^*}, \ldots, b^{d_\ell^*}$ be the successive minima in the dual lattice $\mathcal{R}_\ell^*$ with the distance function $\|\cdot\|_{\mathbf{0}}$. Among the $b^{\ell s}$ boxes of an $(\ell, \ldots, \ell)$-equidissection, $b^{k-d}$ contain exactly $b^d$ points each and the others are empty, where*

$$d = \sum_{m=1}^{\ell} \max(0, d_m^* - s).$$

*In particular, the $s$-dimensional* resolution *is the minimal value of $\ell$ for which $d_1^* \geq s$.*

*Proof.* The proof uses the same argument as in Proposition 4.6 of [34]. Consider the $\ell$-dimensional point set $P_n' = \varphi(\mathcal{R}_\ell) \cap [0,1)^\ell$ obtained by using $\mathcal{R}_\ell$ as a dimensionwise lattice. Observe that the $(\ell, \ldots, \ell)$-equidissection of $P_n$ partitions the points in $\ell s$ boxes in exactly the same way as the $(s, \ldots, s)$-equidissection of $P_n'$. The result then follows by applying Proposition 6 (or Theorem 2 of [3]) to $P_n'$. □

### 4.3 Resolutionwise Walsh series expansion

For $\mathbf{h} \equiv \mathbf{h}(z) = (h_1(z), \ldots, h_\ell(z)) \in (\mathbb{Z}_b[z])^\ell$ and $\mathbf{u} = (u_1, \ldots, u_s) \in [0,1)^s$, where

$$h_q(z) = \sum_{j=0}^{c_q-1} h_{q,j} z^j \quad \text{and} \quad u_j = \sum_{q \geq 1} u_{j,q} b^{-q} \in [0,1),$$

define

$$\langle \mathbf{h}, \mathbf{u} \rangle = \sum_{q=1}^{\ell} \sum_{j=0}^{c_q-1} h_{q,j} u_{j+1,q} \quad \text{in } \mathbb{Z}_b.$$

The *resolutionwise Walsh series expansion* of $f : [0,1)^s \to \mathbb{R}$ is

$$f(\mathbf{u}) = \lim_{\ell \to \infty} \sum_{\mathbf{h} \in (\mathbb{Z}_b[z])^\ell} \check{f}(\mathbf{h}) e^{2\pi\sqrt{-1}\langle \mathbf{h}, \mathbf{u} \rangle / b},$$

with Walsh coefficients

$$\check{f}(\mathbf{h}) = \int_{[0,1)^s} f(\mathbf{u}) e^{-2\pi\sqrt{-1}\langle \mathbf{h}, \mathbf{u} \rangle / b} d\mathbf{u}.$$

**Proposition 11.** *For a resolutionwise polynomial lattice $\mathcal{R}_\ell$,*

$$\frac{1}{n} \sum_{i=0}^{n-1} e^{2\pi\sqrt{-1}\langle \mathbf{h}, \mathbf{u}_i \rangle / b} = \begin{cases} 1 \text{ if } \mathbf{h} \in \mathcal{R}_\ell^*, \\ 0 \text{ otherwise.} \end{cases} \tag{15}$$

*Proof.* Any $\mathbf{u} \in P_n$ can be written as $\mathbf{u} = \psi_s(\mathbf{w}(z))$ where $\mathbf{w}(z) \in \mathcal{R}_s \cap \mathbb{L}_{b,0}^{\ell}$ has coefficients $w_{q,j}$ as in (14), with $w_{q,j} = 0$ for $j < 1$. For $\mathbf{h} \equiv \mathbf{h}(z) \in \mathcal{R}_\ell^*$, we can also write

$$\begin{aligned} \mathbf{h}(z) \cdot \mathbf{w}(z) &= \sum_{q=1}^{\ell} \sum_{j=0}^{c_q-1} h_{q,j} z^j \sum_{i=1}^{\infty} w_{q,i} z^{-i} \\ &= \sum_{q=1}^{\ell} \sum_{\nu=2-c_q}^{\infty} \sum_{j=0}^{c_q-1} h_{q,j} w_{q,j+\nu} z^{-\nu}. \end{aligned} \tag{16}$$

We have that $\mathbf{h} \in \mathcal{R}_\ell^*$ iff $\mathbf{h}(z) \cdot \mathbf{w}(z) \in \mathbb{Z}_b[z]$ for any such $\mathbf{w}(z)$, i.e., iff the coefficient of $z^{-\nu}$ in (16) is zero for all $\nu \geq 1$.

If $\mathbf{h} \in \mathcal{R}_\ell^*$, by taking $\nu = 1$, we obtain that $\langle \mathbf{h}, \mathbf{u} \rangle = 0$ for all $\mathbf{u} \in P_n$, so each term of the sum in (15) equals 1 and this implies the result.

If $\mathbf{h} \notin \mathcal{R}_\ell^*$, then the coefficient of $z^{-\nu}$ in (16) differs from zero for some $\nu$. Consider the linear mapping $\lambda : \mathcal{R}_s \cap \mathbb{F}_{b,0}^{\ell} \to \mathbb{Z}_b$ defined by $\lambda(\mathbf{w}(z)) = \langle \mathbf{h}, \mathbf{u} \rangle$. Because $\mathcal{R}_s \cap \mathbb{F}_{b,0}^{\ell}$ is closed with respect to addition and subtraction, the image of this mapping can be written as $\{0, b/\kappa, 2b/\kappa, \ldots, (\kappa-1)b/\kappa\}$ where $\kappa$ is a positive divisor of $b$. Moreover, each value in the image appears the same

number of times, thanks to the linearity of the mapping. The left side of (15) can then be written as $(1/\kappa)\sum_{j=0}^{\kappa-1}\exp(2\pi\sqrt{-1}\,j/\kappa)$, which equals zero. □

Define $\mathbb{L}^{\infty} = \mathbb{L}\times\mathbb{L}\times\mathbb{L}\times\cdots$ and $(\mathbb{Z}_b[z])^{\infty} = \mathbb{Z}_b[z]\times\mathbb{Z}_b[z]\times\cdots$. One can view the vectors of $\mathbb{L}^{\ell}$ as $\infty$-dimensional by adding an infinite string of zero coordinates. Let $\mathcal{R}_\ell^{*\infty}$ be the dual of $\mathcal{R}_\ell$ in $\mathbb{L}^{\infty}$, which contains all possible extensions of all vectors in $\mathcal{R}_\ell^*$, including all vectors whose first $\ell$ coordinates are zero.

**Proposition 12.** *If the Walsh series expansion* converges absolutely*, then*

$$E_n = \sum_{\mathbf{0}\neq\mathbf{h}\in\mathcal{R}_\ell^{*\infty}} \check{f}(\mathbf{h}).$$

*Proof.* This can be proved by a similar argument as in the proof of proposition 4 of [18]. □

### 4.4 Random digital shifts

To randomize this type of point set, one can generate a random $\mathbf{U}\in[0,1)^s$ and add the first $\delta$ digits of its digital $b$-ary expansion to those of each point of $P_n$. This corresponds to generating a random vector uniformly in $\mathbb{L}_{b,0}^{\delta}$ and adding it to each vector of $\mathcal{R}_\ell$. For $\delta=\ell$, this is a random shift in $\mathbb{L}_b^{\ell}$. For $\delta<\infty$, this gives a biased estimator $Q_n$, because all digits after the first $\ell$ remain zero. The estimator is unbiased if $\delta=\infty$. Using similar arguments as in the proof of Proposition 4 of [18], one can obtain:

**Proposition 13.** *Suppose $\sigma^2<\infty$. Then,*

$$\sigma^2 = \lim_{\ell\to\infty}\sum_{\mathbf{0}\neq\mathbf{h}\in(\mathbb{Z}_b[z])^{\ell}} |\check{f}(\mathbf{h})|^2 = \sum_{\mathbf{0}\neq\mathbf{h}\in(\mathbb{Z}_b[z])^{\infty}} |\check{f}(\mathbf{h})|^2.$$

*For a digitally-shifted resolutionwise PLR with $\delta=\infty$, $\mathrm{E}[Q_n]=\mu$ and*

$$\mathrm{Var}[E_n] = \sum_{\mathbf{0}\neq\mathbf{h}\in\mathcal{R}_\ell^{*\infty}} |\check{f}(\mathbf{h})|^2.$$

Again, the quality of the lattice can be measured by figures of merit of the form (10), with $\mathcal{L}_s^*$ replaced by $\mathcal{R}_\ell^{*\infty}$, and with weights $w(\mathbf{h})$ that depend on how we expect the $|\check{f}(\mathbf{h})|^2$ to behave.

## 5 Links Between PLRs and Digital Nets

### 5.1 Digital nets and $\mathbb{Z}_b$-linear subspaces of $\mathbb{L}_{b,0}^{s}$

To explore the connection between PLRs and digital nets, we start by introducing yet another form of lattice in a space of formal series with coefficients

in $\mathbb{Z}_b$. The points are defined via the mapping $\varphi$, as before. The class of point sets thus constructed will turn out to be equivalent to the class of digital nets.

Select $k$ vectors $\mathbf{c}_1(z), \ldots, \mathbf{c}_k(z)$ in $\mathbb{L}_{b,0}^s$, define

$$\mathcal{C}_s = \left\{ \mathbf{v}(z) = \sum_{i=1}^{k} y_i \mathbf{c}_i(z) \text{ such that } y_i \in \mathbb{Z}_b \text{ for each } i \right\}, \tag{17}$$

and let $P_n = \varphi(\mathcal{C}_s) \subset [0,1)^s$. Observe that $\mathcal{C}_s$ is contained in $\mathbb{L}_{b,0}^s$, so if exactly $t$ of the vectors $\mathbf{c}_1(z), \ldots, \mathbf{c}_k(z)$ are independent over $\mathbb{Z}_b$, then $P_n$ contains $b^t$ distinct points. In what follows, we shall assume that $t = k$, so the $b^k$ points of $P_n$ are all distinct (otherwise, it suffices to eliminate the extra vectors in order to make $k$ equal to $t$).

If we write $\mathbf{c}_i(z) = (c_{i,1}(z), \ldots, c_{i,s}(z))$ where $c_{i,j}(z) = \sum_{\ell=1}^{\infty} c_{\ell,i}^{(j)} z^{-\ell}$, and let $\mathbf{C}^{(j)}$ be the $\infty \times k$ matrix with elements $c_{\ell,i}^{(j)}$, for each $j$, then this method yields exactly the same point set as the digital net in base $b$ with generating matrices $\mathbf{C}^{(1)}, \ldots, \mathbf{C}^{(s)}$. So what we just gave is an alternative definition of a digital net over $\mathbb{Z}_b$, with identity bijections.

The set $\mathcal{C}_s$ is a module over $\mathbb{Z}_b$ (and a vector space in the case where $\mathbb{Z}_b$ is a field), but it is not necessarily the intersection of a polynomial lattice with $\mathbb{L}_{b,0}$, so not every digital net can be seen as a polynomial lattice point set. For example, if $c_{1,i}^{(j)} = 0$ for all $i, j$, then for each $i$, $z\mathbf{c}_i(z)$ is in the intersection of $\mathbb{L}_{b,0}^s$ with the polynomial lattice generated by $\mathbf{c}_1(z), \ldots, \mathbf{c}_k(z)$, but $z\mathbf{c}_i(z) \notin \mathcal{C}_s$ for at least one $i$ (e.g., the one with the largest length $\|z\mathbf{c}_i(z)\|_{\mathbf{0}}$).

Therefore, $P_n = \varphi(\mathcal{C}_s)$ is not the point set of a polynomial lattice in this case. On the other hand, we have the following result:

**Proposition 14.** *The point set $P_n$ of any polynomial integration lattice for which $b$ is prime can be written as a digital net.*

*Proof.* Let $\mathcal{L}_s$ be a polynomial integration lattice. Such a lattice admits a reduced basis in the sense of Minkowski, say $\mathbf{v}_1, \ldots, \mathbf{v}_s$, with successive minima $b^{d_1}, \ldots, b^{d_s}$, where $d_j \leq 0$ for each $j$ and $d_1 + \cdots + d_s = -k$. Consider the set of $k$ vectors $\mathbf{v}_1, \ldots, z^{-d_1}\mathbf{v}_1, \mathbf{v}_2, \ldots, z^{-d_2}\mathbf{v}_2, \ldots \mathbf{v}_s, \ldots, z^{-d_s}\mathbf{v}_s$. These vectors are linearly independent over $\mathbb{Z}_b$, because $\mathbf{v}_1, \ldots, \mathbf{v}_s$ are linearly independent over $\mathbb{Z}_b[z]$, and the set $\mathcal{C}_s$ that they generate via (17) is equal to $\mathcal{L}_s \cap \mathbb{L}_{b,0}$. Thus, the point set $P_n$ of this polynomial integration lattice is the same as $P_n = \varphi(\mathcal{C}_s)$. □

A different (more complicated) proof of this proposition was given in [21] for $b = 2$ and it was shown how to determine the generating matrices $\mathbf{C}^{(j)}$ in terms of a triangular basis (see also [18], section 3.2). The proof given here shows that the $k$ vectors $\mathbf{c}_i(z)$, and thus the generating matrices $\mathbf{C}^{(j)}$, are provided directly by a reduced basis of the polynomial lattice. For the special case of a polynomial lattice $\mathcal{L}_s$ of rank 1 with basis $\mathbf{v}_1(z) = (v_{1,1}(z), \ldots, v_{1,s}(z))$ together with $\mathbf{v}_j(z) = \mathbf{e}_j$ for $j > 1$, where $v_{1,j}(z) = \sum_{\ell=0}^{\infty} v_{1,j,\ell} z^{-\ell}$, one obtains the same digital net by taking $c_{\ell,i}^{(j)} = v_{1,j,\ell+i-1}$, even if the basis is not reduced [18].

### 5.2 Dual space, short dual vectors, and equidistribution

In this section, to avoid complications, we assume that $b$ is a prime, but some of the results may hold for general $b$ as well. In analogy with the dual lattice $\mathcal{L}_s^*$ of $\mathcal{L}_s$, we can define a *dual space* $\mathcal{C}_s^*$ of $\mathcal{C}_s$ by

$$\mathcal{C}_s^* = \{\mathbf{h}(z) \in (\mathbb{Z}_b[z])^s \text{ such that } \mathbf{h}(z) \cdot \mathbf{v}(z) \in \mathbb{Z}_b[z] \text{ for all } \mathbf{v}(z) \in \mathcal{C}_s\}.$$

This set is closed with respect to addition, subtraction, and multiplication by a polynomial of $\mathbb{Z}_b[z]$. It is therefore a polynomial lattice over $\mathbb{Z}_b[z]$, in the sense of (9). Its dual lattice

$$\mathcal{C}_s^{**} = \{\mathbf{v}(z) \in \mathbb{L}_b^s \text{ such that } \mathbf{v}(z) \cdot \mathbf{h}(z) \in \mathbb{Z}_b[z] \text{ for all } \mathbf{h}(z) \in \mathcal{C}_s^*\}$$

is a polynomial integration lattice, equal to the lattice generated (over $\mathbb{Z}_b[z]$) by $\mathcal{C}_s \cup (\mathbb{Z}_b[z])^s$, so it always contains $\mathcal{C}_s$. Its intersection with $\mathbb{L}_{b,0}^s$ equals $\mathcal{C}_s$ iff $P_n = P^+$, where $P_n = \varphi(\mathcal{C}_s)$ and $P^+ = \varphi(\mathcal{L}_s) \cap [0,1)^s$ is the point set of the polynomial integration lattice $\mathcal{L}_s = \mathcal{C}_s^{**}$. We also have $P_n = P^+$ iff $\deg(\det(\mathcal{C}_s^*)) = k$.

Does the lattice $\mathcal{C}_s^*$ tell us about the $\mathbf{q}$-equidistribution of $P_n = \varphi(\mathcal{C}_s)$, as it was the case for the point set $P^+$ of $\mathcal{L}_s$? We know indeed that $P^+$ is $\mathbf{q}$-equidistributed iff $\mathcal{L}_s^* = \mathcal{C}_s^*$ contains *no* $\mathbf{h} \neq \mathbf{0}$ such that $\|\mathbf{h}\|_{-\mathbf{q}} < 1$. If $\mathcal{C}_s^+$ contains such a vector, then some boxes of the $\mathbf{q}$-equidissection contain no point from $P^+$ and thus no point from $P_n$, because $P_n \subseteq P^+$, so $P_n$ cannot be $\mathbf{q}$-equidistributed. Therefore, $\min_{\mathbf{0} \neq \mathbf{h} \in \mathcal{C}_s^*} \|\mathbf{h}\|_{-q} \geq 1$ is a *necessary* condition for the $\mathbf{q}$-equidistribution of $P_n$. However, it is *not* a *sufficient* condition, as shown by the following example.

*Example 4.* Let $b = 2$, $s = 2$, and consider the polynomial integration lattice $\mathcal{L}_s$ with the two basis vectors $\mathbf{v}_1 = (z^{-2}, 0)$ and $\mathbf{v}_2 = (0, z^{-2})$. The dual of this basis is $\mathbf{h}_1 = (z^2, 0)$ and $\mathbf{h}_2 = (0, z^2)$. We have $\det(\mathcal{L}_s^*) = z^4$, so the point set $P^+$ of this lattice has $n = 2^4 = 16$ points. It is actually a two-dimensional rectangular grid with spacing $1/4$. For $\mathbf{q} = (2, 2)$, this point set is $\mathbf{q}$-equidistributed. Now if we take $\mathbf{c}_1 = \mathbf{v}_1$ and $\mathbf{c}_2 = \mathbf{v}_2$ in (17), the point set $P_n = \varphi(\mathcal{C}_s)$ has only four points, which are the points of $P^+$ whose two coordinates are both less than $1/2$. This $P_n$ is obviously *not* $\mathbf{q}$-equidistributed. On the other hand, here $\mathcal{C}_s^* = \mathcal{L}_s^*$ and $\|\mathbf{h}\|_{-\mathbf{q}} \geq 1$ for all nonzero $\mathbf{h} \in \mathcal{L}_s^*$.

The $\mathbf{q}$-equidistribution of $P_n$ can be characterized in a different way as follows. Let $\mathrm{trunc}_{\mathbf{q}} : \mathcal{C}_s \to \mathbb{L}_b^s$ denote the restriction to $\mathcal{C}_s$ of the mapping $\mathrm{trunc}_{\mathbf{q}}$ introduced at the beginning of section 3.7. This mapping is linear over $\mathbb{Z}_b$ and the dimension $d$ of its kernel (in $\mathcal{C}_s$) determines the number of points $b^d$ falling into $B_0$. Again, there are exactly $b^{k-d}$ boxes of the equidissection that contain $b^d$ points each, and all the other boxes are empty. One has $d = k - r$ where $r$ is the rank of the system $\mathrm{trunc}_{\mathbf{q}}(\mathbf{c}_1), \ldots, \mathrm{trunc}_{\mathbf{q}}(\mathbf{c}_k)$. In particular, $P_n$ is $\mathbf{q}$-equidistributed iff $r = q_1 + \cdots + q_s$.

To express $d$ in terms of a shortest nonzero vector, we shall work with a *different* dual space, defined as follows. We first define the (non-commutative) product $\odot$ in $\mathbb{L}_b$ by

$$\left(\sum_{\ell=-\infty}^{w_2} x_\ell z^\ell\right) \odot \left(\sum_{\ell=w_1}^{\infty} y_\ell z^{-\ell}\right) = \sum_{\ell=w_1-1}^{w_2} x_\ell y_{\ell+1}$$

where the latter sum is in $\mathbb{Z}_b$. For vectors $\mathbf{x}(z) = (x_1(z), \ldots, x_s(z))$ and $\mathbf{y}(z) = (y_1(z), \ldots, y_s(s))$ in $\mathbb{L}_b^s$, the product is defined as $\mathbf{x}(z) \odot \mathbf{y}(z) = \sum_{j=1}^s x_j(z) \odot y_j(z)$. We then define *dual space* $\mathcal{C}_s^\perp$ as the null space of $\mathcal{C}_s$ with respect to this product, i.e.,

$$\mathcal{C}_s^\perp = \{\mathbf{h}(z) \in (\mathbb{Z}_b[z])^s \text{ such that } \mathbf{h}(z) \odot \mathbf{v}(z) = 0 \text{ for all } \mathbf{v}(z) \in \mathcal{C}_s\}.$$

The set $\mathcal{C}_s^\perp$ is closed with respect to addition and subtraction, so it is a lattice over $\mathbb{Z}_b$, i.e., can be written as $\mathcal{C}_s^\perp = \{\mathbf{h}(z) = \sum_{j=1}^s x_i \mathbf{h}_j(z)$ such that $x_i \in \mathbb{Z}_b$ for each $i\}$ for some basis $\mathbf{h}_1(z), \ldots, \mathbf{h}_\nu(z)$, where $\nu$ is the dimension. This $\mathcal{C}_s^\perp$ is similar to the null space $\mathcal{C}^\perp$ defined in [29] and to the $\mathcal{C}_s^*$ defined in Eq. (20.17) of [18], except that here it is represented by polynomials instead of vectors with components in $\mathbb{Z}_b$, and our $\mathcal{C}_s^\perp$ is an infinite set whereas the set $\mathcal{C}^\perp$ in [29] is finite.

**Proposition 15.** *One always has* $\mathcal{C}_s^* \subseteq \mathcal{C}_s^\perp$. *Moreover,* $\mathcal{C}_s^\perp = \mathcal{C}_s^*$ *iff* $\mathcal{C}_s = \mathcal{L}_s \cap \mathbb{L}_{b,0}^s$, *iff* $P_n = P^+$.

*Proof.* Let $\mathbf{h}(z) \in \mathcal{C}_s^\perp$ and $\mathbf{v}(z) \in \mathcal{L}_s$ with coordinates $h_j(z) = \sum_{i=0}^{c-1} h_{j,i} z^i$ and $v_j(z) = \sum_{\ell=-w}^{\infty} u_{j,\ell} z^{-\ell}$ for some integers $c$ and $w$. Recall that $\mathbf{h}(z) \in \mathcal{C}_s^*$ iff $\mathbf{h}(z) \cdot \mathbf{v}(z) \in \mathbb{Z}_b[z]$ for all $\mathbf{v}(z) \in \mathcal{C}_s$. By expanding $\mathbf{h}(z) \cdot \mathbf{v}(z)$ and regrouping the corresponding powers of $z$, we find that $\mathbf{h}(z) \cdot \mathbf{v}(z) \in \mathbb{Z}_b[z]$ iff $\sum_{j=1}^s \sum_{i=0}^{c-1} h_{j,i} u_{j,i+\nu} = 0$ in $\mathbb{Z}_b$ for all $\nu \geq 1$. On the other hand, $\mathbf{h}(z) \in \mathcal{C}_s^\perp$ iff the latter sum is zero for $\nu = 1$ and all $\mathbf{v}(z) \in \mathcal{C}_c$. Since this is a weaker condition, we obviously have $\mathcal{C}_s^* \subseteq \mathcal{C}_s^\perp$.

We have $\mathcal{C}_s = \mathcal{L}_s \cap \mathbb{L}_{b,0}^s$ iff for any $\mathbf{v}(z) \in \mathcal{C}_s$ and any integer $\nu \geq 1$, $z^\nu \mathbf{v}(z) \in \mathcal{L}_s \cap \mathbb{L}_{b,0}^s$ implies that $z^\nu \mathbf{v}(z) \in \mathcal{C}_s$. But this holds iff whenever $\sum_{j=1}^s \sum_{i=0}^{c-1} h_{j,i} u_{j,i+\nu} = 0$ for $\nu = 1$ implies that this sum is also 0 for all $\nu \geq 1$. That is, iff $\mathbf{h}(z) \in \mathcal{C}_s^\perp$ implies that $\mathbf{h}(z) \in \mathcal{C}_s^*$. This proves the first "iff." The second one was shown earlier. □

We are now in a position to formulate the analogue of Propositions 4 to 8 for digital nets.

**Proposition 16.** *Let* $P_n = \varphi(\mathcal{C}_s)$. (i) *The point set* $P_n$ *is* $\mathbf{q}$*-equidistributed iff* $\min_{\mathbf{0} \neq \mathbf{h} \in \mathcal{C}_s^\perp} \|\mathbf{h}\|_{-\mathbf{q}} \geq 1$.
(ii) *The resolution of* $P_n$ *is equal to* $\log_b \min_{\mathbf{0} \neq \mathbf{h} \in \mathcal{C}_s^\perp} \|\mathbf{h}\|_{\mathbf{0}}$.
(iii) *The t-value of* $P_n$ *is equal to* $k - s + 1 - \log_b \min_{\mathbf{0} \neq \mathbf{h} \in \mathcal{C}_s^\perp} \|\mathbf{h}\|_\pi$.
(iv) *Propositions 4 and 5 also hold for digital nets if we replace* $\mathcal{L}_s^*$ *by* $\mathcal{C}_s^\perp$.

*Proof.* The first statement can be proved by a similar argument as in the proof of Proposition 6. An alternate method of proof is given in the appendix of [18]. The second statement follows from the first. The third statement is a reformulation of Corollary 1 of [29]. For the fourth one, it suffices to generalize the proof of [18] to an arbitrary $b$. □

## 6 Acknowledgments

This work has been supported by NSERC-Canada grant No. ODGP0110050, NATEQ-Québec grant No. 02ER3218, and a Killam Research Fellowship. The author is very grateful to Harald Niederreiter for his invitation, encouragement, and helpful comments. This paper is largely based on joint work with Christiane Lemieux over the past four years.

## References

1. N. S. Bakhvalov. On the rate of convergence of indeterministic integration processes within the functional classes $w_p^{(l)}$. *Theory of Probability and its Applications*, 7:227, 1962.
2. R. Couture and P. L'Ecuyer. Lattice computations for random numbers. *Mathematics of Computation*, 69(230):757–765, 2000.
3. R. Couture, P. L'Ecuyer, and S. Tezuka. On the distribution of $k$-dimensional vectors for simple and combined Tausworthe sequences. *Mathematics of Computation*, 60(202):749–761, S11–S16, 1993.
4. R. Cranley and T. N. L. Patterson. Randomization of number theoretic methods for multiple integration. *SIAM Journal on Numerical Analysis*, 13(6):904–914, 1976.
5. B. L. Fox. *Strategies for Quasi-Monte Carlo*. Kluwer Academic, Boston, MA, 1999.
6. M. Fushimi. Increasing the orders of equidistribution of the leading bits of the Tausworthe sequence. *Information Processing Letters*, 16:189–192, 1983.
7. P. Hellekalek. On the assessment of random and quasi-random point sets. In P. Hellekalek and G. Larcher, editors, *Random and Quasi-Random Point Sets*, volume 138 of *Lecture Notes in Statistics*, pages 49–108. Springer, New York, 1998.
8. F. J. Hickernell. A generalized discrepancy and quadrature error bound. *Mathematics of Computation*, 67:299–322, 1998.
9. F. J. Hickernell, H. S. Hong, P. L'Ecuyer, and C. Lemieux. Extensible lattice sequences for quasi-Monte Carlo quadrature. *SIAM Journal on Scientific Computing*, 22(3):1117–1138, 2001.
10. W. Hoeffding. A class of statistics with asymptotically normal distributions. *Annals of Mathematical Statistics*, 19:293–325, 1948.
11. S. Joe and I. H. Sloan. Embedded lattice rules for multidimensional integration. *SIAM Journal on Numerical Analysis*, 29:1119–1135, 1992.
12. N. M. Korobov. The approximate computation of multiple integrals. *Dokl. Akad. Nauk SSSR*, 124:1207–1210, 1959. In Russian.

13. G. Larcher. Digital point sets: Analysis and applications. In P. Hellekalek and G. Larcher, editors, *Random and Quasi-Random Point Sets*, volume 138 of *Lecture Notes in Statistics*, pages 167–222. Springer, New York, 1998.
14. G. Larcher, H. Niederreiter, and W. Ch. Schmid. Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration. *Monatshefte für Mathematik*, 121(3):231–253, 1996.
15. P. L'Ecuyer. Maximally equidistributed combined Tausworthe generators. *Mathematics of Computation*, 65(213):203–213, 1996.
16. P. L'Ecuyer. Tables of maximally equidistributed combined LFSR generators. *Mathematics of Computation*, 68(225):261–269, 1999.
17. P. L'Ecuyer and C. Lemieux. Variance reduction via lattice rules. *Management Science*, 46(9):1214–1235, 2000.
18. P. L'Ecuyer and C. Lemieux. Recent advances in randomized quasi-Monte Carlo methods. In M. Dror, P. L'Ecuyer, and F. Szidarovszki, editors, *Modeling Uncertainty: An Examination of Stochastic Theory, Methods, and Applications*, pages 419–474. Kluwer Academic Publishers, Boston, 2002.
19. P. L'Ecuyer and F. Panneton. Construction of equidistributed generators based on linear recurrences modulo 2. In K.-T. Fang, F. J. Hickernell, and H. Niederreiter, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2000*, pages 318–330. Springer-Verlag, Berlin, 2002.
20. C. Lemieux and P. L'Ecuyer. Selection criteria for lattice rules and other low-discrepancy point sets. *Mathematics and Computers in Simulation*, 55(1–3):139–148, 2001.
21. C. Lemieux and P. L'Ecuyer. Randomized polynomial lattice rules for multivariate integration and simulation. *SIAM Journal on Scientific Computing*, 24(5):1768–1789, 2003.
22. A. K. Lenstra. Factoring multivariate polynomials over finite fields. *Journal of Computer and System Sciences*, 30:235–248, 1985.
23. K. Mahler. An analogue to Minkowski's geometry of numbers in a field of series. *Annals of Mathematics*, 42(2):488–522, 1941.
24. K. Mahler. On a theorem in the geometry of numbers in a space of Laurent series. *Journal of Number Theory*, 17:403–416, 1983.
25. H. Niederreiter. Low discrepancy point sets. *Monatshefte für Mathematik*, 102:155–167, 1986.
26. H. Niederreiter. Low-discrepancy point sets obtained by digital constructions over finite fields. *Czechoslovak Math. Journal*, 42:143–166, 1992.
27. H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*, volume 63 of *SIAM CBMS-NSF Regional Conference Series in Applied Mathematics*. SIAM, Philadelphia, 1992.
28. H. Niederreiter. The existence of good extensible polynomial lattice rules. *Monatshefte für Mathematik*, 139:295–307, 2003.
29. H. Niederreiter and G. Pirsic. Duality for digital nets and its applications. *Acta Arithmetica*, 97:173–182, 2001.
30. A. B. Owen. Latin supercube sampling for very high-dimensional simulations. *ACM Transactions of Modeling and Computer Simulation*, 8(1):71–102, 1998.
31. I. H. Sloan and S. Joe. *Lattice Methods for Multiple Integration*. Clarendon Press, Oxford, 1994.
32. S. Tezuka. A new family of low-discrepancy point sets. Technical Report RT-0031, IBM Research, Tokyo Research Laboratory, Jan. 1990.

33. S. Tezuka. The $k$-dimensional distribution of combined GFSR sequences. *Mathematics of Computation*, 62(206):809–817, 1994.
34. S. Tezuka. *Uniform Random Numbers: Theory and Practice*. Kluwer Academic Publishers, Norwell, Mass., 1995.
35. S. Tezuka and P. L'Ecuyer. Efficient and portable combined Tausworthe random number generators. *ACM Transactions on Modeling and Computer Simulation*, 1(2):99–112, 1991.