*Les Cahiers du GERAD* ISSN: 0711–2440

# A Coding Theoretic Approach to Building Nets with Well-Equidistributed Projections

Y. Edel
P. L'Ecuyer

G–2007–19

March 2007

# A Coding Theoretic Approach to Building Nets with Well-Equidistributed Projections

**Yves Edel**

*Mathematisches Institut der Universität*
*Im Neuenheimer Feld 288*
*69120 Heidelberg, Germany*
y.edel@mathi.uni-heidelberg.de

**Pierre L'Ecuyer**

*GERAD and*
*Département d'informatique et de recherche opérationnelle*
*Université de Montréal*
*C.P. 6128, Succ. Centre-ville*
*Montréal (Québec) Canada, H3C 3J7*
*and IRISA, Rennes, France*
lecuyer@iro.umontreal.ca

March 2007

*Les Cahiers du GERAD*
G–2007–19

**Abstract**

Starting from coding-theoretic constructions, we build digital nets with good figures of merit, where the figure of merit takes into account the equidistribution of a preselected set of low-dimensional projections. This type of figure of merit turns out to be a better predictor than the $t$-value for the variance of randomized quasi-Monte Carlo (RQMC) estimators based on nets, for certain classes of integrals. Our construction method determines the most significant digits of the points by exploiting the equivalence between the desired equidistribution properties used in our criterion and the property of a related point set to be an orthogonal array, and using existing orthogonal array constructions. The least significant digits are then adjusted to improve the figure of merit. Known results on orthogonal arrays provide bounds on the best possible figure of merit that can be achieved. We present a concrete construction that belongs to the class of cyclic digital nets and we provide numerical illustrations of how it can reduce the variance of an RQMC estimator, compared with more standard constructions.

**Résumé**

Partant de structures issues de la théorie des codes, nous construisons des réseaux digitaux dont les mesures de qualité sont excellentes, lorsque ces mesures prennent en compte l'équidistribution d'un ensemble choisi de projections de l'ensemble de points sur des sous espaces de petites dimensions. Ce type de mesure de qualité s'avère un meilleur prédicteur que la $t$-valeur pour la variance d'estimateurs de type quasi-Monte Carlo randomisés (RQMC) basés sur les réseaux digitaux, pour certaines classes d'intégrales. Nos méthodes de construction déterminent d'abord les digits les plus significatifs des coordonnées des points en exploitant l'équivalence entre les propriétés d'équidistribution visées par les mesures de qualité et la propriété d'un ensemble de points légèrement modifié d'être un tableau orthogonal, et en utilisant des méthodes de construction connues pour les tableaux orthogonaux. Les digits les moins significatifs sont ensuite ajustés pour améliorer les mesures de qualité. À partir de résultats connus sur les tableaux orthogonaux, on peut obtenir des bornes sur les meilleures valeurs possibles pour les mesures de qualité. Nous présentons une construction concrète qui appartient à la classe de réseaux digitaux cycliques. Nous donnons des exemples numériques pour illustrer la réduction de variance obtenue par un estimateur RQMC qui utilise ces réseaux, en comparaison avec d'autres réseaux digitaux connus.

**Acknowledgments:** This research has been supported by NSERC-Canada grant No. ODGP0110050 and a Canada Research Chair to the second author.

# 1 Introduction

This paper deals with the construction of finite sets of points that are more evenly distributed in the $s$-dimensional unit hypercube, in some sense, than a typical set of random points. The two main issues that arise in building such point sets are: (a) to define an appropriate measure of uniformity, or measure of *discrepancy* between the uniform distribution and the empirical distribution of the points; (b) to find construction methods for point sets having high uniformity, or low discrepancy, with respect to the retained definition.

A popular class of construction is that of digital nets [16, 18], whose uniformity is usually measured by figures of merit defined in terms of the equidistribution of the points in certain families of rectangular boxes that partition the unit hypercube. A widely-used figure of merit in this context is the $t$-value [13, 16, 18, 23, 24]. One limitation of this measure, however, is that when the dimension of the point set is much larger than the basis of the net, the $t$-value is necessarily large, and it does not really take into account the quality of the low-dimensional projections. There are several applications in RQMC integration where for a given $t$-value, the uniformity of certain low-dimensional projections can make an important difference [11, 15, 22].

The aim of this paper is to propose digital net constructions with good $t$-values and high-quality low-dimensional projections and to exhibit theoretical bounds on what can be achieved in this direction. We do this by exploiting the links between digital net constructions on the one hand, and some established results on orthogonal arrays and error correcting codes on the other hand. Results from coding theory have already been exploited extensively to construct digital nets with a small $t$-value and to compute tables of the best known $t$-value for a given dimension, basis, and number of points [4, 17, 18, 24]. Here we use similar techniques to define skeletons for our nets, i.e., to determine the most significant digits of the points. The construction is then refined by adjusting the least significant digits to improve our figure of merit. Known results on orthogonal arrays also provide bounds on the best possible figure of merit that can be achieved.

As a concrete example, we propose an algebraic construction of a family of cyclic digital nets with well-equidistributed projections. These nets are *cyclic* in the sense that if we shift all coordinates of any given $s$-dimensional point of the net by one position to the left and put the old first coordinate at the end, the resulting point is always in the net. (This definition differs from that of [17].) By repeating the blocks of $s$ successive coordinates ad infinitum, these nets provide point sets that are infinite-dimensional and dimension-stationary, in the sense of [11, 22]. We present a family of cyclic $(t, m, s)$-nets that belong to that class; they have the same parameters $t$, $m$, and $s$ as in [4] (which give the best

$t$ known so far for certain values of $s$ and $m$), and improved equidistribution properties for certain projections. We give a numerical illustration showing that this type of point set can be more accurate than other well-established digital nets (such as Sobol' nets) for QMC integration, at least for certain types of integrands.

The rest of the paper is organized as follows. In Section 2, we recall and discuss various ways of measuring the uniformity of digital nets. In Section 3, we make the links between the nets that we want to construct and orthogonal arrays, whose additive versions are the duals of additive error-correcting codes. A specific class of cyclic net constructions is proposed and analyzed in Section 4. The numerical illustrations are in Section 5.

## 2 Digital Nets and Their Figures of Merit

**QMC and RQMC.** We want to construct finite point sets of the form $P_n = \{\mathbf{u}_0, \ldots, \mathbf{u}_{n-1}\}$ in $[0,1)^s$ with *low discrepancy* (i.e., *high uniformity*) in some sense.. These point sets can be used, for instance, to estimate the integral of some function $f$ over $[0,1)^s$ by quasi-Monte Carlo (QMC):

$$\mu = \int_{[0,1)^s} f(\mathbf{u}) d\mathbf{u} \approx \frac{1}{n} \sum_{i=0}^{n-1} f(\mathbf{u}_i). \tag{1}$$

*Randomized QMC* (RQMC) also uses the approximation (1), but after randomizing the point set $P_n$ in a way that each individual point has the uniform distribution over $[0,1)^s$ even though the point set as a whole keeps its high uniformity [13, 16, 20]. It has the advantage of providing an unbiased estimator of $\mu$, and also an unbiased variance estimator if we make several independent randomizations.

**Digital nets.** The two most widely used classes of constructions for $P_n$ are digital nets and lattice rules [16, 26]. We focus on the former. For given integers $b \geq 2$ (usually a prime or a prime power) and $m \geq 1$, a *digital net in base* $b$ with $n = b^m$ points is defined as follows. For $j = 1, \ldots, s$, select a $w \times m$ *generator matrix* $\mathbf{C}^{(j)}$ whose elements are either in the finite ring $\mathbb{Z}_b$ or in the finite field $\mathbb{F}_b$. (If $b = p^e$ where $p$ is prime and $e > 1$, the operations in $\mathbb{F}_b$ and in $\mathbb{Z}_b$ are not equivalent, so one must make sure that the correct arithmetic is used, depending on how the $\mathbf{C}^{(j)}$ where constructed.) To define the $i$th point $\mathbf{u}_i$, for $i = 0, \ldots, b^m - 1$, we write the digital expansion of $i$ in base $b$ and multiply the vector of its digits by $\mathbf{C}^{(j)}$, modulo $b$, to obtain the digits or the expansion of $u_{i,j}$, the $j$th coordinate of $\mathbf{u}_i$. That is,

$$
\begin{aligned}
i &= a_{i,0} + a_{i,1}b + \cdots + a_{i,m-1}b^{m-1}, \\
\begin{pmatrix} u_{i,j,1} \\ u_{i,j,2} \\ \vdots \end{pmatrix} &= \mathbf{C}^{(j)} \begin{pmatrix} a_{i,0} \\ a_{i,1} \\ \vdots \\ a_{i,m-1} \end{pmatrix} \\
u_{i,j} &= \sum_{\ell=1}^{\infty} u_{i,j,\ell} b^{-\ell}, \qquad \mathbf{u}_i = (u_{i,1}, \ldots, u_{i,s}).
\end{aligned}
$$

In practice, we take $w$ and $m$ finite, but there is no limit on their size. If the generating matrices are defined with an infinite number of columns, then we have a *digital sequence* of points. If we have an infinite sequence of generating matrices, then the points can be thought as having infinite dimension. Typically, these infinite sequences are defined via recurrences, either for the successive columns or the successive generating matrices. Well-known digital net constructions are those of Sobol', Faure, Niederreiter, and Niederreiter-Xing.

**Equidistribution.** Let $(q_1, \ldots, q_s)$ be a vector of nonnegative integers such that $q = q_1 + \ldots + q_s \leq m$. A $(q_1, \ldots, q_s)$-*equidissection in base* $b$ is a partition of the unit hypercube in $b^{q_1+\cdots+q_s}$ rectangular boxes aligned with the axes, of equal volume $b^{-q}$, defined by dividing the interval $[0, 1)$ along the $j$-th coordinate into $b^{q_j}$ equal parts, for each $j$. A point set $P_n$ with $n = b^m$ is said to be $(q_1, \ldots, q_s)$-*equidistributed in base* $b$ if every cell defined by the $(q_1, \ldots, q_s)$-equidissection contains exactly $b^{m-q}$ points from $P_n$. It is easy to see that a digital net in base $b$ is $(q_1, \ldots, q_s)$-equidistributed in base $b$ if and only if the matrix constructed with the first $q_1$ rows of $\mathbf{C}^{(1)}$, the first $q_2$ rows of $\mathbf{C}^{(2)}$, ..., and the first $q_s$ rows of $\mathbf{C}^{(s)}$, has full rank $q_1 + \cdots + q_s$. This is possible only if $q_1 + \cdots + q_s \leq m$.

These definitions apply more generally to lower-dimensional projections of $P_n$. For $I = \{i_1, \ldots, i_\eta\} \subseteq \{1, \ldots, s\}$, $P_n(I)$ denotes the $\eta$-dimensional *projection* of $P_n$ on the coordinates determined by $I$. The set $P_n(I)$ is $(q_{i_1}, \ldots, q_{i_\eta})$-*equidistributed in base* $b$ if each box of the $(q_{i_1}, \ldots, q_{i_\eta})$-equidissection has the same number of points. This is equivalent to saying that $P_n$ is $(\tilde{q}_1, \ldots, \tilde{q}_s)$-equidistributed with $\tilde{q}_j = q_{i_h}$ if $j = i_h \in I$ and $\tilde{q}_j = 0$ otherwise. This equidistribution can thus be verified by checking the rank of a matrix as explained earlier.

**The $t$-value.** A digital net in base $b$ with $n = b^m$ points is a $(t, m, s)$-*net in base* $b$, also denoted $(t, m, s)_b$ net, if it is $(q_1, \ldots, q_s)$-equidistributed whenever $q_1 + \cdots + q_s \leq m - t$ [16]. The smallest integer $t \geq 0$ such that this holds is called the $t$-*value* of the net. Ideally, we want $t$ to be as small as possible. But $t = 0$ is possible only if $s \leq b + 1$ [16]. Otherwise,

the best possible $t$-value can be much larger than 0; the best possible $t$-value as a function of $b$ and $s$, together with the best known $t$-values, can be found in the `MinT` tables of [24].

For example, in base $b = 2$, for $m = 14$ and $s = 23$, the best known $t$-value is $t = 8$. This guarantees equidistribution only for $q_1 + \cdots + q_s \leq 6$, i.e., when considering no more than 6 output bits. But why not be more demanding for low-dimensional projections? For instance, an easily achieved requirement would be that all one-dimensional projections be $(m)$-equidistributed. We could also ask that other low-dimensional projections have a smaller $t$-value; in the previous example where $t = 8$, for instance, we may ask that several of the two-dimensional projections have a $t$-value of 0.

Another way to compromise when the lower bound on the $t$-value is deemed too high is to define a figure of merit that takes the worst case over a smaller number of equidissections, i.e., fewer shapes of boxes. This is the direction we take in what follows.

**Looking at square boxes only.** We say that $P_n$ or $P_n(I)$ is *$\eta$-distributed with $\ell$ digits of accuracy* if it is $(\ell, \ldots, \ell)$-equidistributed. This means that if we partition the hypercube into $b^{\eta\ell}$ cubic boxes or equal size, each box contains exactly $b^{m-\eta\ell}$ points. The largest $\ell$ for which this holds is the *$\eta$-dimensional resolution of $P_n(I)$ in base $b$*, denoted $\ell(I)$. One has $\ell(I) \leq \lfloor m/\eta \rfloor$. The *resolution gap of $P_n(I)$* is defined by $\delta(I) = \lfloor m/\eta \rfloor - \ell(I)$. This can be used to define a worst-case criterion based on (cubic) equidistribution [12, 13]:

$$\Delta_{\mathcal{J}} = \max_{I \in \mathcal{J}} \delta(I)$$

where $\mathcal{J}$ is a selected class of sets $I \subseteq \{1, \ldots, s\}$. The choice of $\mathcal{J}$ is arbitrary. If $\mathcal{J}$ contains too many projections, typically there are inevitably some bad ones and the criterion loses its discriminatory power, because it only cares about the worst projections. A leaner $\mathcal{J}$ can concentrate on the most important projections, if it diminishes the theoretical lower bound on $\Delta_{\mathcal{J}}$. As a practical compromise, Lemieux and L'Ecuyer [13] suggested the form

$$\begin{aligned} \mathcal{J} \;=\; & \{\{0, 1, \ldots, i\} : i < s_1\} \cup \; \{\{i_1, i_2\} : 0 = i_1 < i_2 < s_2\} \cup \cdots \\ & \cup \{\{i_1, \ldots, i_d\} : 0 = i_1 < \ldots < i_d < s_d\} \end{aligned} \tag{2}$$

for arbitrarily selected values of $d, s_1, \ldots, s_d$.

## 3 A Coding Theoretic Link: Orthogonal Arrays

An *orthogonal array* $\mathrm{OA}(n, s, q, t)$ is an array of $n$ rows and $s$ columns, with entries in $\{0, 1, \ldots, q-1\}$, such that in the submatrix formed by any $t$ columns of the array, each of the $q^t$ possibilities for a row appear equally often, namely $n/q^t$ times each. We say that we have an orthogonal array (OA) with $n$ *words* (or *runs*), *length* $s$ (or $s$ *factors*), $q$ *levels*, and *strength* $t$. For further details on OAs, see [3, 6, 19].

We can define a correspondence between an OA and a point set $P_n$ in $[0,1)^s$ simply by dividing each entry of the array by $q$ and viewing each row of the array as representing an $s$-dimensional point. With a slight abuse of language, we also call this point set an OA (i.e., identify it with the OA). Note that all coordinates of all points in this point set are multiples of $1/q$. If $q = b^\ell$ for some positive integers $b$ and $\ell$, the OA$(n, s, q, t)$ property means that every $t$-dimensional projection of $P_n$ is $t$-distributed with $\ell$ digits of accuracy, in base $b$.

Let $\mathcal{J}_\eta$ denotes the class of all subsets of exactly $\eta$ coordinates, i.e., of the form $I = \{i_1, \ldots, i_\eta\} \subseteq \{1, \ldots, s\}$. If $P_n$ is a point set whose coordinates are all multiples of $b^{-\ell}$, then $P_n$ is an OA$(n, s, b^\ell, \eta)$ if and only if

$$\min_{I \in \mathcal{J}_\eta} \ell(I) \geq \ell,$$

if and only if

$$\Delta_{\mathcal{J}_\eta} \leq \lfloor m/\eta \rfloor - \ell.$$

If $P_n$ is a *digital* net with $n = b^m$ where $b$ is prime, then the sum (digitwise, modulo $b$) of two points of the net is again a point of the net; that is, the corresponding OA is an *additive* OA, which is the *dual* of an *additive error-correcting code* $(s, b^{\ell s - m}, \eta + 1)_{b^\ell}$ [3, 6]. In fact, each additive error-correcting code gives an additive orthogonal array, and vice-versa.

Our aim here is to construct digital nets $P_n$ in base $b$, such that $P_n$ truncated to its first $\ell_\eta$ digits is an OA$(b^m, s, b^{\ell_\eta}, \eta)$, *simultaneously* for $\eta = 1, 2, \ldots, d$, where each $\ell_\eta$ *is as large as possible*. So our task is more than just looking up for existing OAs or codes. A trivial upper bound for each $\ell_\eta$ is $\ell_\eta \leq \lfloor m/\eta \rfloor$. Known bounds on the largest $\ell$ for which there can exist an OA$(b^m, s, b^\ell, \eta)$ are generally tighter than this trivial bound. In some cases, there are known constructions that match the bounds. Note that the closer $\eta$ is to $s/2$, the more $\eta$-dimensional projections there are. To verify the OA property, $\eta\ell$ digits of each projection are examined, so a larger $\ell$ means that more digits are involved (the boxes have smaller volume) and the corresponding OA is then harder to construct.

***Example 1*** Take $b = 2$, $s = 65$, and $m = 12$, so $n = 2^{12}$. Table 1 gives upper bounds on the largest $\ell$ for which there can be an OA$(2^{12}, 65, 2^\ell, \eta)$, as well as the values of $\ell$ achieved by known OA constructions.

The upper bounds from `MinT` [24] are obtained as follows. For $\eta = 3$ there is no OA$(16^3, 19, 2^4, 3)$ which is a consequence of the bound on OAs with index unity [5]. For $\eta = 4$, from the linear programming bound we find that there is no OA$(4^6, 30, 2^2, 4)$ [25]. For $\eta = 5$, there is no OA$(2^{12}, 65, 2, 5)$, because otherwise its truncation would provide an OA$(2^{11}, 64, 2, 4)$, which would violate the sphere-packing bound [3].

The best known additive OAs, on the other hand, can be found from the best known linear error-correcting codes $[65, 65 - 12/\ell, \eta + 1]_{2^\ell}$. For the case $\eta = 1$, there is an obvious

Table 1: Upper bounds on the values of $\ell$ for which there can exist an $\mathrm{OA}(2^{12}, 65, 2^\ell, \eta)$, and values for which there exist known constructions.

| $\eta$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | $\cdots$ | 12 |
|---|---|---|---|---|---|---|---|---|---|
| $\lfloor 12/\eta \rfloor$ | 12 | 6 | 4 | 3 | 2 | 2 | 1 | $\cdots$ | 1 |
| `MinT` upper bound for OA | | | 3 | 1 | 0 | 0 | 0 | $\cdots$ | 0 |
| Best known additive OA | 12 | 6 | 3 | 1 | 0 | 0 | 0 | $\cdots$ | 0 |
| Best known net | 12 | 6 | 3 | 1 | 0 | 0 | 0 | $\cdots$ | 0 |

construction. For $\eta = 2$, there is a Hamming code $[65, 65-2, 3]_{64}$. For $\eta = 3$, there is an ovoid code $[65, 65-4, 4]_8$. For $\eta = 4$, there is a binary linear code $[65, 53, 5]_2$.

Our strategy for building our nets will be to start with a good (known) $\mathrm{OA}(n, s, b^\ell, \eta)$ for some reasonably large $\eta$ (and a rather small $\ell$, necessarily) and fix the first $\ell$ digits of the net; then, in a second stage, we "optimize" the other digits, either by algebraic construction or via computer search, to obtain a point set whose $\ell(\eta')$-digit truncation is an $\mathrm{OA}(n, s, b^{\ell(\eta')}, \eta')$ for reasonably large $\ell(\eta')$, for all $\eta' \le \eta$.

# 4 A Cyclic Net Construction

We call a digital net $P_n$ *cyclic* if for any point $(u_0, \ldots, u_{s-2}, u_{s-1}) \in P_n$, we also have $(u_1, \ldots, u_{s-1}, u_0) \in P_n$. For a cyclic digital net $P_n$, whenever $b$ is prime and $\gcd(b, s) = 1$, the net is a direct product of rings (principal ideal domains). These rings turn out to be linear cyclic codes, one of the favorite classes of codes of coding theorists, and their structure can be exploited for efficient computer search and algebraic constructions of good instances of these nets. The following special case illustrates this.

**A cyclic net construction.** The following construction gives a cyclic digital net $P_n$ in base $b = 2$, with $n = 2^{4r}$ points in $s = 2^{2r} + 1$ dimensions, for some integer $r$. The dimensions of the generating matrices will be $w = m = 4r$. This net can be used to approximate integrals in $s' \le s$ dimensions by taking only the first $s'$ coordinates of each point. For $s' > s$, we can take advantage of the cyclic property to get as many coordinates as needed. The periodicity of the coordinates will be destroyed by the randomization (see Section 5).

The generator matrices of the net are defined as follows. Recall that

$$\mathbb{F}_2 \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^{2r}} \subset \mathbb{F}_{2^{4r}}.$$

Let $\zeta \in \mathbb{F}_{2^{4r}}$ be a $(2^{2r}+1)$th primitive root of unity, i.e., such that $\zeta^{2^{2r}+1} = 1$. Such a $\zeta$ exists because we know that there is an element $\zeta'$ of multiplicative order $2^{4r} - 1$, so

it suffices to take $\zeta = (\zeta')^{2^{2r}-1}$, which has multiplicative order $2^{2r}+1$. Choose a basis $1 = \alpha_1, \ldots, \alpha_r$ of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$ and choose some elements $\beta \in \mathbb{F}_{2^{2r}} \setminus \mathbb{F}_{2^r}$, and $\gamma \in \mathbb{F}_{2^{4r}} \setminus \mathbb{F}_{2^{2r}}$. Put

$$a_i = \alpha_i, \quad a_{i+r} = \beta\alpha_i, \quad a_{i+2r} = \gamma\alpha_i, \quad a_{i+3r} = \gamma\beta\alpha_i,$$

for $i = 1, \ldots, r$. Then, $a_1, \ldots, a_r$ form a basis of $\mathbb{F}_{2^r}$, $a_1, \ldots, a_{2r}$ are a basis of $\mathbb{F}_{2^{2r}}$, and $a_1, \ldots, a_{4r}$ are a basis of $\mathbb{F}_{2^{4r}}$.

To define the $i$th row of the matrix $\mathbf{C}^{(j)}$, we compute $a_i\zeta^j \in \mathbb{F}_{2^{4r}}$ and represent it as a vector of $4r$ elements (or coordinates) over $\mathbb{F}_2$.

**Proposition 1** *For $r > 1$, the cyclic net just constructed has the following properties:*

*(i) It is a digital $(4r-4, 4r, 2^{2r}+1)$-net in base 2*

*(ii) It is $(4r)$-equidistributed for all one-dimensional projections.*

*(iii) It is $(2r, 2r)$-equidistributed for all two-dimensional projections.*

*(iv) It is $(r, r, r)$-equidistributed for all three-dimensional projections..*

*(v) It is $(1, 1, 1, 1)$-equidistributed for all four-dimensional projections.*

*(vi) It is $(1, \ldots, 1)$-equidistributed whenever $I = \{j, j+1, \ldots, j+4r-1\}$.*

*(vii) It is $(r, r, r, r)$-equidistributed whenever $I = \{j, j+1, j+2, j+3\}$ or $I = \{j, k, l, m(j,k,l)\}$, for any pairwise different $j, k, l$ and some $2^r - 2$ different $m(j,k,l)$. Thus, the proportion of four-dimensional projections that are $(r, r, r, r)$-equidistributed is approximately $1/(1 - 1/n^2)$.*

**Proof.** That the net is $(4r)$-equidistributed for all one-dimensional projections is equivalent to the fact that the matrix $\mathbf{C}^{(j)}$ has full rank. This is obvious, as the $\alpha_i, \beta\alpha_i, \gamma\alpha_i, \gamma\beta\alpha_i$ are a basis of $\mathbb{F}_{2^{4r}}$ over $\mathbb{F}_2$ and $\zeta^j \neq 0$.

Now we want to show that the net is $(2r, 2r)$-equidistributed for all two-dimensional projections. We have to show that the first $2r$ rows of $\mathbf{C}^{(j)}$ and the first $2r$ rows of $\mathbf{C}^{(j')}$ have full rank. The first $2r$ rows of $\mathbf{C}^{(j)}$ are of the form $a_i\zeta^j$ and the $a_i$, for $1 \leq i \leq 2r$, are a basis of $\mathbb{F}_{2^{2r}}$. So we have to show that $\zeta^j$ and $\zeta^{j'}$ are linearly independent over $\mathbb{F}_{2^{2r}}$. Let $W = \{\zeta^j | 0 \leq j < 2^{2r}+1\} \subset \mathbb{F}_{4^r}$ be the group of elements of multiplicative order $2^{2r}+1$. As $\gcd(2^{2r}+1, 2^{2r}-1) = 1$, we have that $W \cap \mathbb{F}_{2^{2r}} = \{1\}$. So two different $\zeta^j, \zeta^{j'} \in W$ are linearly independent over $\mathbb{F}_{2^{2r}}$.

For the $(r, r, r)$-equidistribution, with the same argument, we have to show the linear independence of different powers of $\zeta$ over $\mathbb{F}_{2^r}$. It is known, that the $(2^{2r}+1)$-th roots of unity, i.e., $W$ is an ovoid in $\mathrm{PG}(3, 2^r)$, where $\mathrm{PG}(k, q)$ denotes the $k$-dimensional projective geometry over the finite field $\mathbb{F}_q$ [3, 7] (see the proof of Theorem 17 of [2]). The defining property of the ovoid implies that the $\zeta^j \in W$ are a $\mathbb{F}_{2^r}$-linear OA of strength 3. This

means that for any distinct indexes $\{j, j', j''\}$, $\zeta^j, \zeta^{j'}, \zeta^{j''}$ are linearly independent over $\mathbb{F}_{2^r}$. Hence the net is $(r, r, r)$-equidistributed for all three-dimensional projections.

For the $(r, r, r, r)$-equidistribution we consider again the $\zeta^j$ as *points* in $PG(3, 2^r)$ (not to be confused with the points of $P_n$). Consider four points $\zeta^j, \zeta^k, \zeta^l, \zeta^{m(j,k,l)}$. Since $W$ is an ovoid and three independent points define a plane in $PG(3, 2^r)$, the points $\zeta^{m(j,k,l)}$ that are not independent from $\{\zeta^j, \zeta^k, \zeta^l\}$ are those points of the ovoid that lie in the plane generated by $\{\zeta^j, \zeta^k, \zeta^l\}$. The claimed property follows from the fact that every plane that contains more than one point of the ovoid in $PG(3, 2^r)$ contains exactly $2^r + 1$ points of the ovoid (Theorem 16.1.6.ii in [7]).

That the net is $(r, r, r, r)$-equidistributed for $I = \{j, j+1, j+2, j+3\}$ follows from the fact that $\{1, \zeta, \zeta^2, \zeta^3\}$ are linearly independent over $\mathbb{F}_{2^r}$, because $\mathbb{F}_{2^{4r}}$ is the smallest field that contains $\zeta$. That the net is $(1, \ldots, 1)$-equidistributed whenever $I = \{j, j+1, \ldots, j+4r-1\}$ follows from the fact that $\{1, \zeta, \ldots, \zeta^{4r-1}\}$ are linearly independent over $\mathbb{F}_2$.

The net is $(1, 1, 1, 1)$-equidistributed for all four-dimensional projections. This follows from the fact that the binary code we obtain by restriction to the first digit has strength 4; see [4] for the proof.

For the $(t, m, s)$-net property (i), we have to show that the net is $(l_1, l_2, l_3, l_4)$-equidistributed whenever $l_1 + l_2 + l_3 + l_4 = 4$. The only case that is not covered by what we already have shown is the $(3, 1)$-equidistribution for all two dimensional projections, for $r = 2$. But for $r = 2$ we are exactly in the same situation as in [4], where the corresponding $(t, m, s)$-net property is proved. □

## 5 Numerical Illustrations

We report (a subset of) the results of numerical experiments where we try our cyclic nets for estimating some multivariate integrals by RQMC. We compare their performance with that of Sobol' nets when both are randomized by a random binary digital shift [13, 21]. In each case, we estimate the variance per run, defined as $n$ times the variance of the average over the $n$ points, and compare it with the empirical variance of standard Monte Carlo (MC). The *variance reduction factor* (VRF) reported is the ratio of the MC variance over the RQMC variance per run. The digital nets are randomized by a random digital shift (DS), which consists in generating a single point $\mathbf{u} = (u_1, \ldots, u_s)$ uniformly over $[0, 1)^s$, and performing a digit-wise addition modulo $b$ of $u_j$ with the $j$th coordinate of each point of $P_n$, for each $j$. For $b = 2$, the digit-wise addition becomes a bitwise exclusive-or. This randomization preserves the equidistribution for every equidissection in base 2; in particular, it preserves the $(t, m, s)$-net properties. The primitive polynomials and the direction numbers for the Sobol' sequence were taken from [14].

***Example 2*** This example is from [9] and [22]. We consider the function $f$ defined by

$$f(u_1, \ldots, u_s) = \sqrt{\frac{2}{t(t-1)}} \sum_{j=0}^{t-1} \sum_{i=0}^{j-1} g(u_i) g(u_j),$$

where $g(x) = 27.20917094x^3 - 36.19250850x^2 + 8.983337562x + 0.7702079855$ and $s = 120$. We take $n$ from $2^{14}$ to $2^{16}$ and we use RQMC with 100 independent digital random shifts (DS) to estimate the variance for each method. Table 2 gives the VRF for different digital nets. The $\mathbb{F}_{2^w}$ nets were proposed by Panneton and L'Ecuyer [22]; these authors tried 12 instances of these nets on this example and obtained VRFs ranging from 10 to $4 \times 10^5$. With the $(0, 2, 126)_{125}$-net, we obtain a competitive VRF. (Note that this net cannot be written as a net in base 2.) These $(0, 2, q+1)_q$-nets are essentially the duals of Hamming codes. They provide an optimal resolution for the projections in one and two dimensions, which seems to be what we need for the function $f$ considered here. With the net from Proposition 1, with $r = 4$, we obtain a significantly larger VRF.

***Example 3*** This example is from [8] and [10]. We consider a Bermudan-Asian option on $c$ assets. For $1 \le i \le c$, the value of asset $i$ evolves as a geometric Brownian motion (GMB) $\{S_i(t),\, t \ge 0\}$ with *drift parameter* $\mu_i$ and *volatility parameter* $\sigma_i$. That is,

$$S_i(t) = S_i(0) \exp\left[(\mu_i - \sigma_i 2/2)t + \sigma_i W_i(t)\right]$$

where $W_i$ is a standard Brownian motion. The $W_i$'s are also correlated, with $\mathrm{Cov}\,[W_i(t+\delta) - W_i(t),\, W_j(t+\delta) - W_j(t)] = \rho_{i,j}\delta$ for all $\delta > 0$. The option has discounted payoff $e^{-rT} \max[\bar{S}^{(\mathrm{A})} - K,\, 0]$ for some constants $K > 0$ and $T > 0$, where

$$\bar{S}^{(\mathrm{A})} = \frac{1}{cd} \sum_{i=1}^{c} \sum_{j=1}^{d} S_i(t_j) \tag{3}$$

Table 2: Variance reduction factors of RQMC compared with MC, with various digital nets.

| net | $n$ | VRF |
|---|---|---|
| Sobol | $2^{14}$ | 2 |
| Sobol | $2^{16}$ | 2 |
| $\mathbb{F}_{2^w}$-nets | $2^{14} - 2^{16}$ | 10 to $4 \times 10^5$ |
| $(0, 2, 129)_{128}$-net | $2^{14}$ | 330 |
| $(0, 2, 126)_{125}$-net | $5^6$ | $8.3 \times 10^4$ |
| Proposition 1 | $2^{16}$ | $1.8 \times 10^6$ |

is the arithmetic average at the fixed observation times $t_j = jT/d$ for $j = 1, \ldots, d$. The vector $\mathbf{Y} = (W_1(t_1), \ldots, W_c(t_1), W_1(t_2), \ldots, W_c(t_2), \ldots, W_1(t_d), \ldots, W_c(t_d))^{\mathsf{t}}$, has a multivariate normal distribution with mean zero and covariance matrix $\boldsymbol{\Sigma}$ whose element $((i-1)c+j), (i'-1)c+j')$ is $\rho_{i,i'}\sigma_i\sigma_{i'}|t_{j'} - t_{j-1}|)$ for $j' \geq j$.

To generate $\mathbf{Y}$, we can decompose $\boldsymbol{\Sigma}$ as $\boldsymbol{\Sigma} = \mathbf{C}\mathbf{C}^{\mathsf{t}}$ for some matrix $\mathbf{C}$, generate a vector $\mathbf{Z} = (Z_1, \ldots, Z_s)$ of independent $N(0,1)$ (standard normal) random variates by inversion from $s$ independent $U(0,1)$ random variates $U_1, \ldots, U_s$, i.e., $Z_j = \Phi^{-1}(U_j)$, and return $\mathbf{Y} = \mathbf{C}\mathbf{Z}$. There are several possibilities for the choice of factorization $\boldsymbol{\Sigma} = \mathbf{C}\mathbf{C}^{\mathsf{t}}$. For instance, the *Cholesky factorization*, takes $\mathbf{C}$ lower triangular, whereas *principal component analysis* (PCA) selects $\mathbf{C}$ so that each $Z_j$ accounts for the maximum amount of variance conditional on $Z_1, \ldots, Z_{j-1}$. Its combination with QMC was suggested in [1].

We take the same parameters as in Example 2 of [10]: $c = 10$, $d = 25$ (so $s = 250$), $\rho_{i,j} = 0.4$ for all $i \neq j$, $T = 1$, $\sigma_i = 0.1 + 0.4(i-1)/9$ for all $i$, $r = 0.04$, $S(0) = 100$, and $K = 100$. We thus have a 250-dimensional integral. Simulations with a huge number of runs told us that $\mu \approx 5.818$ and the MC variance is $\sigma^2 \approx 72.3$.

Recall that the Sobol' nets are constructed to behave well for the projections over the first successive coordinates, but not for arbitrary projections over coordinates with a large index, whereas the net of Proposition 1 has been built precisely to have good uniformity for projections over a small number of arbitrary coordinates. With the Cholesky decomposition, the variance is spread over pretty much all coordinates, whereas PCA pushes most of the variance in the first coordinates. Thus, we expect the Sobol' nets to work well when PCA is used and the new nets to be more competitive if one is forced to use the Cholesky decomposition. The simulation results reported in Table 3 agree with these expectations. We also tried with different values of $r$, from 0.03 to 0.07, and the VRFs were similar. The VRFs are much larger with PCA than with Cholesky, due to the fact that PCA reduces significantly the effective dimension in the truncation sense [8, 13]. But PCA is not always practical for real-life problems; for instance when the dimension is very large. Then, one may have to use more traditional simulation schemes that do not reduce the effective dimension in the truncation sense. The new nets can be useful in this type of situation.

Table 3: Empirical variance reduction factors of RQMC with respect to MC for Example 3 (in 250 Dimensions), for a Sobol' net and for the net of Proposition 1, with $n = 2^{16}$ points.

| net | Cholesky | PCA |
|---|---|---|
| Sobol' | 16 | 6144 |
| Proposition 1 | 50 | 2108 |

## References


[1] P. Acworth, M. Broadie, and P. Glasserman. A comparison of some Monte Carlo and quasi-Monte Carlo techniques for option pricing. In P. Hellekalek, G. Larcher, H. Niederreiter, and P. Zinterhof, editors, *Monte Carlo and Quasi-Monte Carlo Methods 1996*, volume 127 of *Lecture Notes in Statistics*, pages 1–18. Springer-Verlag, New York, 1998.

[2] J. Bierbrauer. Large caps. *Journal of Geometry*, 76:16–51, 2003.

[3] J. Bierbrauer. *Introduction to Coding Theory*. Chapman and Hall/CRC Press, Boca Raton, FL, USA, 2004.

[4] J. Bierbrauer and Y. Edel. Construction of digital nets from BCH-codes. In P. Hellekalek, G. Larcher, H. Niederreiter, and P. Zinterhof, editors, *Monte Carlo and Quasi-Monte Carlo Methods 1996*, volume 127 of *Lecture Notes in Statistics*, pages 221–231. Springer-Verlag, New York, 1998.

[5] K. A. Bush. Orthogonal arrays of index unity. *Annals of Mathematical Statistics*, 13:426–434, 1952.

[6] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer-Verlag, New York, 1999.

[7] J. W. P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Clarendon Press, Oxford, 1985.

[8] J. Imai and K. S. Tan. Enhanced quasi-Monte Carlo methods with dimension reduction. In E. Yücesan, C. H. Chen, J. L. Snowdon, and J. M. Charnes, editors, *Proceedings of the 2002 Winter Simulation Conference*, pages 1502–1510, Piscataway, New Jersey, 2002. IEEE Press.

[9] L. Kocis and W. J. Whiten. Computational investigations of low-discrepancy sequences. *ACM Transactions on Mathematical Software*, 23(2):266–294, June 1997.

[10] P. L'Ecuyer. Quasi-Monte Carlo methods in finance. In R. G. Ingalls, M. D. Rossetti, J. S. Smith, and B. A Peters, editors, *Proceedings of the 2004 Winter Simulation Conference*, Piscataway, New Jersey, 2004. IEEE Press.

[11] P. L'Ecuyer and C. Lemieux. Quasi-Monte Carlo via linear shift-register sequences. In *Proceedings of the 1999 Winter Simulation Conference*, pages 632–639. IEEE Press, 1999.

[12] P. L'Ecuyer and C. Lemieux. Variance reduction via lattice rules. *Management Science*, 46(9):1214–1235, 2000.

[13] P. L'Ecuyer and C. Lemieux. Recent advances in randomized quasi-Monte Carlo methods. In M. Dror, P. L'Ecuyer, and F. Szidarovszky, editors, *Modeling Uncertainty: An Examination of Stochastic Theory, Methods, and Applications*, pages 419–474. Kluwer Academic, Boston, 2002.

[14] C. Lemieux, M. Cieslak, and K. Luttmer. *RandQMC User's Guide: A Package for Randomized Quasi-Monte Carlo Methods in C*, 2004. Software user's guide, available at `http://www.math.ucalgary.ca/~lemieux/`.

[15] 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.

[16] 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.

[17] H. Niederreiter. Digital nets and coding theory. In K. Q. Feng, H. Niederreiter, and C. P. Xing, editors, *Coding, Cryptography and Combinatorics*, volume 23 of *Progress in Computer Science and Applied Logic*, pages 247–257. Birkhäuser, Basel, 2004.

[18] H. Niederreiter. Constructions of $(t, m, s)$-nets and $(t, s)$-sequences. *Finite Fields and Their Applications*, 11:578–600, 2005.

[19] A. B. Owen. Orthogonal arrays for computer experiments, integration and visualization. *Statistica Sinica*, 2(2):439–452, 1992.

[20] A. B. Owen. Latin supercube sampling for very high-dimensional simulations. *ACM Transactions on Modeling and Computer Simulation*, 8(1):71–102, 1998.

[21] A. B. Owen. Variance with alternative scramblings of digital nets. *ACM Transactions on Modeling and Computer Simulation*, 13(4):363–378, 2003.

[22] F. Panneton and P. L'Ecuyer. Infinite-dimensional highly-uniform point sets defined via linear recurrences in $F_{2^w}$. In H. Niederreiter and D. Talay, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2004*, pages 419–429, Berlin, 2006. Springer-Verlag.

[23] G. Pirsic and W. Ch. Schmid. Calculation of the quality parameter of digital nets and application to their construction. *Journal of Complexity*, 17(4):827–839, 2001.

[24] W. Ch. Schmid and R. Schürer. MinT, the database for optimal $(t, m, s)$-net parameters. `http://mint.sbg.ac.at`, 2005.

[25] R. Schürer and W. Ch. Schmid. Linear programming bounds; in MinT, the database for optimal $(t, m, s)$-net parameters. `http://mint.sbg.ac.at/desc_CBoundLP.html`, version: 2006-12-20, 2006.

[26] I. H. Sloan and S. Joe. *Lattice Methods for Multiple Integration*. Clarendon Press, Oxford, 1994.