(t, m, s)-Nets and Maximized Minimum Distance, Part II

Leonhard Grünschloß and Alexander Keller

Abstract The quality parameter t of (t, m, s)-nets controls extensive stratification properties of the generated sample points. However, the definition allows for points that are arbitrarily close across strata boundaries. We continue the investigation of (t, m, s)-nets under the constraint of maximizing the mutual distance of the points on the unit torus and present two new constructions along with algorithms. The first approach is based on the fact that reordering (t, s)-sequences can result in $(t, m, s+1)$-nets with varying toroidal distance, while the second algorithm generates points by permutations instead of matrices.

1 Introduction

Important problems in image synthesis like e.g. anti-aliasing, hemispherical integration, or the illumination by area light sources can be considered as low-dimensional numerical integration problems. Among the most successful approaches to computing this kind of integrals are quasi-Monte Carlo and randomized quasi-Monte Carlo methods [9, 13, 2] based on the two-dimensional Larcher-Pillichshammer points [10], which expose a comparatively large minimum toroidal distance.

These points belong to the class of (t, m, s)-nets in base q (for an extensive overview of the topic we refer to [12, Ch. 4, especially p. 48]), which is given by

Leonhard Grünschloß
mental images GmbH, Fasanenstraße 81, 10623 Berlin, Germany.
email: `leonhard@gruenschloss.org`

Alexander Keller
mental images GmbH, Fasanenstraße 81, 10623 Berlin, Germany.
email: `alex@mental.com`

Definition 1. For integers $0 \le t \le m$, a (t,m,s)-*net in base* q is a point set of q^m points in $[0,1)^s$ such that there are exactly q^t points in each elementary interval E with volume q^{t-m}.

Figure 1 shows an instance of a $(0,4,2)$-net in base 2 and illustrates the concept of *elementary intervals*

$$E = \prod_{i=1}^{s} \left[a_i q^{-b_i}, (a_i+1) q^{-b_i}\right) \subseteq [0,1)^s$$

as used in the definition, where $a_i, b_i \in \mathbb{Z}$, $b_i \ge 0$ and $0 \le a_i < q^{b_i}$. The concept of (t,m,s)-nets can be generalized for sequences of points as given by

Definition 2. For an integer $t \ge 0$, a sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $[0,1)^s$ is a (t,s)-*sequence in base* q if, for all integers $k \ge 0$ and $m > t$, the point set $\mathbf{x}_{kq^m}, \ldots, \mathbf{x}_{(k+1)q^m-1}$ is a (t,m,s)-net in base q.

Obviously, the stratification properties of (t,m,s)-nets and (t,s)-sequences are best for the quality parameter $t=0$, because then every elementary interval contains exactly one point, as illustrated in Figure 1. The conception does not consider the mutual distance of the points, which allows points to lie arbitrarily close together across shared interval boundaries.

In this paper we continue previous work from [6] that used the *minimum toroidal distance*

$$d_{\min}\left(\{\mathbf{x}_0, \ldots, \mathbf{x}_{N-1}\}\right) := \min_{0 \le u < v < N} \|\mathbf{x}_u - \mathbf{x}_v\|_T$$

to classify point sets $\{\mathbf{x}_0, \ldots, \mathbf{x}_{N-1}\}$, where the toroidal distance of two points $\mathbf{x} = (x_1, \ldots, x_s) \in [0,1)^s$ and $\mathbf{y} = (y_1, \ldots, y_s) \in [0,1)^s$ is defined as

$$\|\mathbf{x} - \mathbf{y}\|_T := \sqrt{\sum_{i=1}^{s} \left(\min\{|x_i - y_i|, 1 - |x_i - y_i|\}\right)^2}.$$

Maximizing the shift-invariant measure of toroidal distance further increases uniformity, allows one to tile the resulting point sets, and to consider periodic integrands, which is especially useful in the aforementioned graphics applications.

In Section 2 we therefore extend the construction of Larcher and Pillichshammer to $s=3$ dimensions resulting in a $(0,m,3)$-net in base 2, which exhibits a large minimum toroidal distance. In Section 3 we then present a new permutation-based construction for $(0,m,2)$-nets in base 2, which often have a larger minimum toroidal distance than can be obtained by any digital net in base 2.

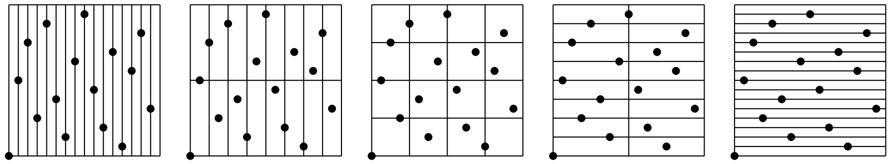


Fig. 1 The Larcher-Pillichshammer points as an example of a $(0, 4, 2)$-net in base 2 superimposed on all possible elementary intervals. There is exactly one point in each elementary interval.

2 A new $(0, m, 3)$-Net in Base 2 with Large Minimum Toroidal Distance

Although both the Hammersley and Larcher-Pillichshammer points are constructions of $(0, m, 2)$-nets in base 2, the latter have a much larger minimum toroidal distance [8]. In fact already in [10, 11] the Hammersley points have been identified to be the worst construction with respect to certain other measures, too.

The extension of the Larcher-Pillichshammer points to $s = 3$ dimensions has been an open problem for long. In the following, we present a construction of a $(0, m, 3)$-net in base 2, where one two-dimensional projection equals the Larcher-Pillichshammer points [9] and therefore benefits from their large minimum toroidal distance.

2.1 Digital Nets and Sequences

We briefly summarize necessary notation and algorithmic facts on digital nets and sequences from [12] in a simplified manner. While in general digital nets and sequences are defined using a finite field $\mathbb{F}_q$, with q being a prime power, we only consider the case $q = 2$ in the following.

Given suitable $m \times m$-matrices $C_1, \ldots, C_s$ over $\mathbb{F}_2$, the i-th component of the n-th point for $1 \le i \le s$ and $0 \le n < 2^m$ can be generated by

$$x_n^{(i)} = \begin{pmatrix} 2^{-1} \\ \vdots \\ 2^{-m} \end{pmatrix}^T \left[C_i \begin{pmatrix} d_0(n) \\ \vdots \\ d_{m-1}(n) \end{pmatrix} \right] \in [0, 1),$$

where the matrix-vector multiplication has to be performed in $\mathbb{F}_2$ and the digits $d_k(n)$ are defined by the binary expansion of

$$n = \sum_{k=0}^{m-1} d_k(n) 2^k.$$

The elements of the i-th generator matrix are denoted by $c_{j,r}^{(i)}$.

The theoretical construction of (t,s)-sequences requires generator matrices of infinite size. However, in practice this does not pose a problem when enumerating the points, since $d_k(n) = 0$ for all sufficiently large k and, in addition, we require the matrix entries $c_{j,r}^{(i)} = 0$ for all sufficiently large j [12, p. 72, (S6)]. Therefore, only finite upper left submatrices have to be considered when generating points. Finally, due to the finite precision of integer computation, m is finite in any case.

Based on the results in [10, 11, 4], we will consider the $(0,1)$-sequence in base 2 generated by the non-singular upper triangular matrix

$$C_1' := \left(\begin{cases} 1 & \text{if } j \le r, \\ 0 & \text{otherwise} \end{cases} \right)_{j,r=0}^{\infty} \tag{1}$$

in order to generate the Larcher-Pillichshammer points [9].

2.2 Reordering the Sobol'-Sequence

We now take a look at the first two components of the Sobol'-sequence [15], which are a $(0,2)$-sequence in base 2, and are defined by the infinite upper triangular matrices

$$C_1 := (\delta_{j,r})_{j,r=0}^{\infty} \quad \text{and} \quad C_2 := \left(\binom{r}{j} \bmod 2 \right)_{j,r=0}^{\infty},$$

where $\delta_{j,r} = 1$ for $j = r$ and zero otherwise. In the above definition and the remainder of this work, by $a \bmod m$ we mean the *common residue*. That is the nonnegative value $b < m$, such that $a \equiv b \mod m$.

Suppose that the infinite matrices $C_1, \ldots, C_s$ over $\mathbb{F}_2$ generate a $(0,s)$-sequence in base 2. Furthermore suppose that the infinite matrix C_1' over $\mathbb{F}_2$ generates a $(0,1)$-sequence in base 2. This implies that C_1' is a nonsingular upper triangular matrix. Then a $(0,s)$-sequence in base 2 is generated by $C_1', C_2 D, \ldots, C_s D$, where $D := C_1^{-1} C_1'$. This new sequence consists of the same points as before, however, in a different order. This result is proven in more general form in [5, Prop. 1].

Note that the first generator matrix C_1' is the one of Larcher-Pillichshammer. Since C_1 is the identity, we have $D = C_1^{-1} C_1' = C_1'$ and obtain

$$\begin{aligned} C_2 D &= \left(\binom{r}{j} \bmod 2 \right)_{j,r=0}^{\infty} C_1' \\ &= \left(\sum_{k=0}^{r} \binom{k}{j} \bmod 2 \right)_{j,r=0}^{\infty} \\ &= \left(\binom{r+1}{j+1} \bmod 2 \right)_{j,r=0}^{\infty} =: C_2', \end{aligned} \tag{2}$$

as the second generator matrix, where the last equality follows from the Christmas Stocking Theorem.

Note that the same reordering can be applied to the Faure-sequence [3], which can be regarded as a generalization of the Sobol'-sequence for any prime base q. An even more general construction for any prime power base can be found in [12].

2.3 Construction

Combining the component $\frac{n}{2^m}$ with the first 2^m points of a $(0, 2)$-sequence in base 2 yields a $(0, m, 3)$-net in base 2 (see [12, Lemma 4.22, p. 62]). The relationship of C_1' and C_2' as expressed in Equation (2) in fact is a property of all $(0, 2)$-sequences in base 2 generated by non-singular upper triangular matrices [7, Prop. 4]. Consequently fixing the first generator matrix uniquely determines the second generator matrix and thus the $(0, m, 3)$-net.

In the previous section we reordered the Sobol'-sequence in base 2 such that one component matches the $(0, 1)$-sequence as defined in [10]. For the construction of the new $(0, m, 3)$-net in base 2, it is sufficient to consider the matrices C_1', C_2' from Section 2.2, because for $s = b = 2$ Sobol's construction is identical to Faure's construction. By construction two dimensions of the resulting three-dimensional net are the Larcher-Pillichshammer points [9].

In Figure 2 we compared the minimum toroidal distance of the new construction to the one that uses the original Sobol' generator matrices C_1 and C_2. Except for $m = 5$ and $m = 6$, the new construction is by far superior for all $m \leq 22$. We did not compute the minimum toroidal distance for $m > 22$, though.

2.3.1 Implementation

The following code in `C99` (the current ANSI standard of the `C` language) returns the n-th point of the $(0, m, 3)$-net generated using C_1' and C_2' (see Equations (1) and (2)) for $m < 32$ in $\mathcal{O}(m)$. The vectorized implementa-

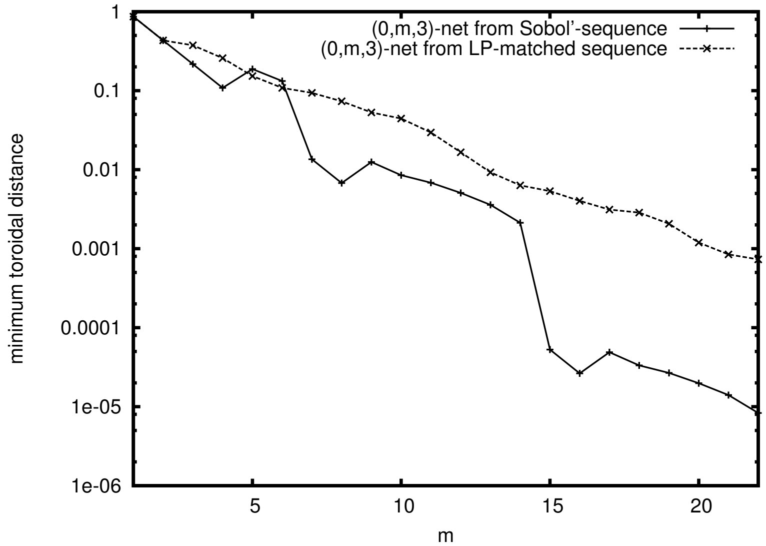


Fig. 2 A plot of the toroidal distance in $[0,1)^3$ for both the Sobol' $(0,m,3)$-net as well as the $(0,m,3)$-net constructed using C_1', C_2', where one of the two-dimensional projections equals the Larcher-Pillichshammer point set. We would like to stress that the minimum distance is scaled logarithmically, so the absolute difference is very significant for increasing m. In contrast to the Sobol'-net, the minimum distance decreases smoothly for the new construction.

tion is based on the fact that addition in $\mathbb{F}_2$ corresponds to the *exclusive or* operation.

```
void x_n(unsigned int n, const unsigned int m, float x[3]) {
  // first component: n / 2^m
  x[0] = (float) n / (1U << m);

  // remaining components by matrix multiplication
  unsigned int r1 = 0, r2 = 0;
  for (unsigned int v1 = 1U << 31, v2 = 3U << 30; n; n >>= 1) {
    if (n & 1) { // vector addition of matrix column by XOR
      r1 ^= v1;
      r2 ^= v2 << 1;
    }
    // update matrix columns
    v1 |= v1 >> 1;
    v2 ^= v2 >> 1;
  }

  // map to unit cube [0,1)^3
  x[1] = r1 * (1.f / (1ULL << 32));
  x[2] = r2 * (1.f / (1ULL << 32));
}
```

3 Permutation-Generated $(0, m, 2)$-Nets in Base 2 with Larger Minimum Toroidal Distance

Taking the integer part of the coordinates of a $(0, m, s)$-net in base q multiplied by the number of points q^m results in each component being a permutation from the symmetric group S_{q^m}. For $s = 2$ dimensions and base $q = 2$ this is visualized in Figure 1, where each column and each row (the leftmost and rightmost set of elementary intervals in the figure) contain exactly one point.

Using Heap's efficient permutation generation algorithm [14] allows one to enumerate all permutations $\pi : \{0, \ldots, 2^m - 1\} \to \{0, \ldots, 2^m - 1\}$ that represent $(t, m, 2)$-nets in base 2 with the points $\frac{1}{2^m}(n, \pi(n)) \in [0, 1)^2$. We extended this basic backtracking algorithm by pruning the search tree whenever the elementary-interval property $t = 0$ was violated or already a net with larger minimum toroidal distance than the current one had been found. Verifying the $t = 0$ property is simple using the code published in [6, Section 2.2].

Performing such an exhaustive combinatorial computer search seems hopeless given the number of possible permutations $|S_{2^m}| = (2^m)!$ and in fact we did not succeed in running an exhaustive search for $m > 5$. In these cases we simply generated random permutations, but kept the backtracking approach mentioned above.

However in [6], we were able to find very regular looking $(0, 5, 2)$-nets with a minimum toroidal distance of $\sqrt{32}/2^5 \approx 0.17677670$, which is larger than the minimum toroidal distance of all possible digital $(0, 5, 2)$-nets, where the maximum is $\sqrt{29}/2^5 \approx 0.1682864$.

In continuation of these findings we now present a first construction (see Figure 3) of such permutation-based nets. In Table 1 we compare the minimum toroidal distance of different $(0, m, 2)$-nets in base 2. The new permutation construction clearly features the largest minimum toroidal distance. Due to the novelty of the approach, we present two different derivations and provide more interpretations than usually necessary.

3.1 Iterative Construction by Quadrupling Point Sets

Given the search results as displayed in Figure 3, an iterative construction procedure can be inferred. This procedure repeatedly quadruples an initial point set until the desired number of 2^m points is reached. We therefore need to distinguish the cases of even and odd m as depicted by the examples in Figure 4.

We represent the $(0, k, 2)$-nets in base 2 by

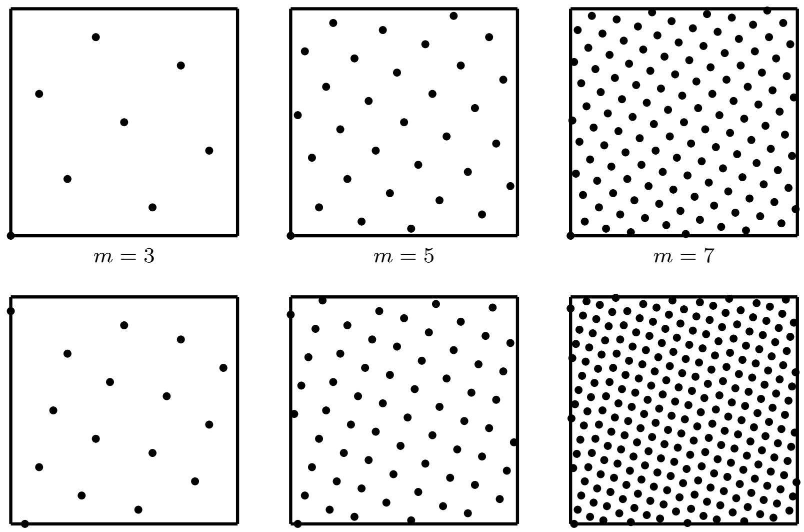


Fig. 3 Examples of the permutation-generated $(0, m, 2)$-nets in base 2 for $m = 3, \ldots, 8$.

m	Hammersley	Larcher-Pillichsh.	Opt. matrices	Permutation
2	2	2	2	2
3	2	5	8	8
4	2	8	13	13
5	2	18	29	32
6	2	32	52	53
7	2	72	100	128
8	2	128	208	241
9	2	265	400	512
10	2	512	832	964
11	2	1060	1600	2048
12	2	2048	3328	3856
13	2	4153	6385	8192
14	2	8192	13312	15424
15	2	16612	25313	32768
16	2	32768	53248	61696

Table 1 Comparison of the Hammersley points, the Larcher-Pillichshammer points, the points resulting from the optimized matrices given in [6], and the new permutation construction with respect to minimum toroidal distance. Note that for easier comparison all distances have been multiplied by the number 2^m of points of a $(0, m, 2)$-net in base 2 and squared afterwards.

$$\left\{ \frac{1}{2^k}(u \bmod 2^k, v) : (u, v) \in P_k \right\}, \tag{3}$$

where the set P_k contains 2^k integer coordinates (u, v).

For odd m the initial point set P_1 consists of the points $(0, 0)$ and $(1, 1)$. The quadrupling rule to construct a point set $P_{k+2} := P_{k,0} \cup P_{k,1} \cup P_{k,2} \cup P_{k,3}$ with 2^{k+2} points from a point set P_k with $|P_k| = 2^k$ points is as follows:

$$\begin{aligned}
\text{Lower left:} \quad & P_{k,0} := \{(2u, 2v) : \ (u, v) \in P_k\} \\
\text{Lower right:} \quad & P_{k,1} := \left\{(2^{k+1} + 2u + 1, 2v + 1) : \ (u, v) \in P_k\right\} \\
\text{Upper left:} \quad & P_{k,2} := \left\{(2^{k+1} + 2u, 2^{k+1} + 2v) : \ (u, v) \in P_k\right\} \\
\text{Upper right:} \quad & P_{k,3} := \left\{(2^{k+2} + 2u + 1, 2^{k+1} + 2v + 1) : \ (u, v) \in P_k\right\}
\end{aligned}$$

For even m, the iterative construction is more involved. We start out with four diagonals, each consisting of four points:

$$\begin{aligned}
P_{2,0} &:= \{(w + 1, 4w) : \ w = 0, \ldots, 3\}, \\
P_{2,1} &:= \{(w + 5, 4w + 2) : \ w = 0, \ldots, 3\}, \\
P_{2,2} &:= \{(w + 9, 4w + 1) : \ w = 0, \ldots, 3\}, \\
P_{2,3} &:= \{(w + 13, 4w + 3) : \ w = 0, \ldots, 3\}.
\end{aligned}$$

The quadrupling rule for even k constructs $P_{k+2} := P'''_{k,0} \cup P'''_{k,1} \cup P'''_{k,2} \cup P'''_{k,3}$ from sets $P_{k,l}$ for $l = 0, \ldots, 3$ as follows:

1. Multiply all points by two and add an offset for the points in P_1 and P_3:

$$P'_{k,l} := \{(2u + (l \bmod 2), 2v) : \ (u, v) \in P_{k,l}\} \ \text{ for } l = 0, \ldots, 3.$$

2. Extend the diagonals:

$$P''_{k,l} := P'_{k,l} \cup \left\{(2^{k-1} + u, 2^{k+1} + v) : \ (u, v) \in P'_{k,l}\right\} \ \text{ for } l = 0, \ldots, 3.$$

3. Combine diagonals:

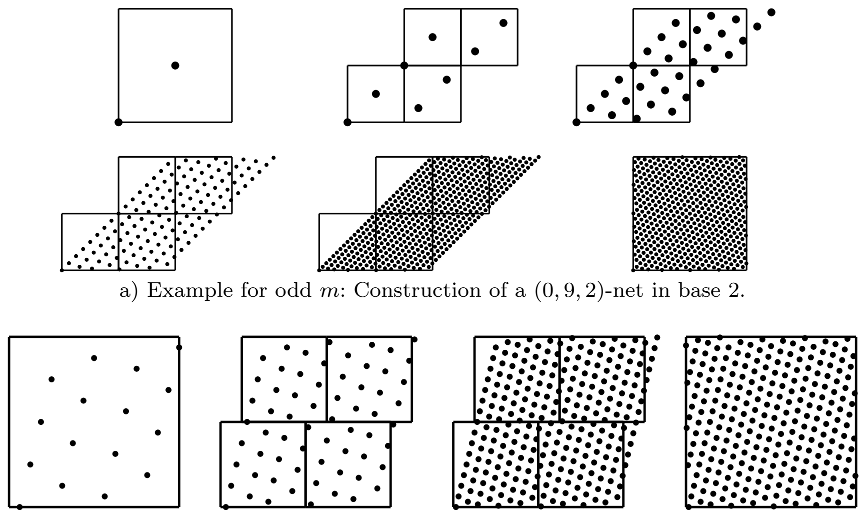
$$\begin{aligned}
P'''_{k,0} &:= P''_{k,0} \cup P''_{k,1}, \\
P'''_{k,1} &:= P''_{k,2} \cup P''_{k,3}.
\end{aligned}$$

4. Append shifted copies:

$$\begin{aligned}
P'''_{k,2} &:= \left\{(2^{k+1} + u, u + 1) : \ (u, v) \in P'''_{k,0}\right\}, \\
P'''_{k,3} &:= \left\{(2^{k+1} + v, v + 1) : \ (u, v) \in P'''_{k,1}\right\}.
\end{aligned}$$

3.2 Direct Construction

As these nets consist of points lying on parallel diagonals similar to rank-1 lattices [2], a direct construction is possible by computing a single point on



a) Example for odd m: Construction of a $(0,9,2)$-net in base 2.

b) Example for even m: Construction of a $(0,8,2)$-net in base 2.

Fig. 4 Iterative construction of $(0,m,2)$-nets in base 2 by quadrupling point sets, where the final net results from wrapping the points such that they match the unit square. This wrapping corresponds to the modulo operation in Equation (3).

each diagonal. Since the points are evenly spaced along the diagonals, the remaining points follow immediately. These diagonals are to be understood with a modulo 2^m wrap-around for the first coordinate.

3.2.1 Construction for Odd m

The position of the point with the smallest second coordinate on the d-th diagonal is given by $(2^m \phi_2(d) + d, d)$, where $0 \le d < 2^{\lfloor \frac{m}{2} \rfloor}$ and $\phi_2(d) \in [0,1)$ denotes the van der Corput radical inverse in base 2.

Theorem 1. *For odd m, the points*

$$\left\{ (u_{d,w}, v_{d,w}) : 0 \le d < 2^{\lfloor \frac{m}{2} \rfloor}, 0 \le w < 2^{\lceil \frac{m}{2} \rceil} \right\},$$

where

$$u_{d,w} = \left(2^m \phi_2(d) + d + w \cdot 2^{\lfloor \frac{m}{2} \rfloor} \right) \bmod 2^m, \tag{4}$$

$$v_{d,w} = d + w \cdot 2^{\lfloor \frac{m}{2} \rfloor}, \tag{5}$$

constitute a $(0,m,2)$-net in base 2 with a minimum toroidal distance of $\sqrt{2^m}$. This distance is measured using components multiplied by 2^m, i.e. on integer scale.

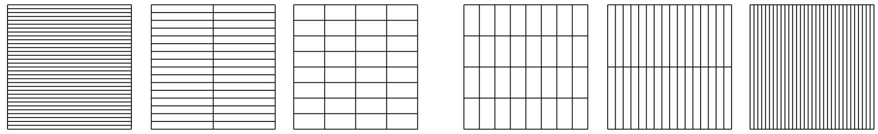


Fig. 5 The two cases in the proof corresponding to certain kinds of elementary intervals, illustrated here for $m = 5$.

Proof. First, we will show that the elementary interval property holds. For each kind $0 \le h \le m$ of elementary intervals, there must be exactly one point in each integer-scaled elementary interval

$$\left[x \cdot 2^h, (x+1)2^h\right) \times \left[y \cdot 2^{m-h}, (y+1)2^{m-h}\right),$$

where $0 \le x < 2^{m-h}$ and $0 \le y < 2^h$. Partitioning the set of elementary intervals as depicted in Figure 5, we need to consider two cases:

1. We first consider the case $\left\lceil \frac{m}{2} \right\rceil \le h \le m$. The width of these kinds of elementary intervals is larger than their height. Looking at Equation (5), we can see that the $\left\lfloor \frac{m}{2} \right\rfloor$ least significant bits of $v_{d,w}$ are equal to the bits of d, while the remaining $\left\lceil \frac{m}{2} \right\rceil$ most significant bits of $v_{d,w}$ are equal to the bits of w. Considering one horizontal strip of elementary intervals, y determines the h most significant bits of $v_{d,w}$. Since $h \ge \left\lceil \frac{m}{2} \right\rceil$, w is completely determined by y. What remains to show is that for this fixed w, the $m - h$ most significant bits of $u_{d,w}$ differ for suitable values for d. Analyzing Equation (4), we see that the term $w \cdot 2^{\left\lfloor \frac{m}{2} \right\rfloor}$ is constant, while the addition of d only modifies the $\left\lfloor \frac{m}{2} \right\rfloor$ least significant bits. However
$$\left\{2^m \phi_2(d) :\ 0 \le d < \left\lfloor \frac{m}{2} \right\rfloor\right\} = \left\{d \cdot \left\lceil \frac{m}{2} \right\rceil :\ 0 \le d < \left\lfloor \frac{m}{2} \right\rfloor\right\}, \qquad (6)$$
thus due to the addition of $2^m \phi_2(d)$ it is possible to guarantee that the $\left\lfloor \frac{m}{2} \right\rfloor \ge m-h$ most significant bits of $u_{d,w}$ are different by selecting suitable values for d. Thus the corresponding points fall into different elementary intervals.
2. Now we consider the case $0 \le h \le \left\lfloor \frac{m}{2} \right\rfloor$. The width of these kinds of elementary intervals is smaller than their height. We consider one vertical strip of elementary intervals of width 2^h. Looking at Equation (4), we can see that the the only way to achieve consecutive values $u_{d,w}$ equal to $x, x+1, \ldots, x+2^h-1$ is by using consecutive values for d. That is because the terms $2^m \phi_2(d)$ and $w \cdot 2^{\left\lfloor \frac{m}{2} \right\rfloor}$ do not modify the $h \le \left\lfloor \frac{m}{2} \right\rfloor$ least significant bits of $u_{d,w}$. However 2^h consecutive values for d mean that the $h \le \left\lfloor \frac{m}{2} \right\rfloor$ most significant bits of the values $2^m \phi_2(d)$ are different for each d (cf. to Equation (6)). In order to stay in the vertical strip of elementary intervals determined by x, the h most significant bits of w thus must be

chosen accordingly for each point inside this strip in order to "compensate" using the term $w \cdot 2^{\lfloor \frac{m}{2} \rfloor}$. As a consequence of the different values for w it follows from Equation (5) that the $h \leq \lceil \frac{m}{2} \rceil$ most significant bits of $v_{d,w}$ are different for each point inside this strip, thus they fall into different elementary intervals.

We now consider the achieved minimum toroidal distance of the point set. Points on the diagonals are placed with a multiple of the offset $\left(2^{\lfloor \frac{m}{2} \rfloor}, 2^{\lfloor \frac{m}{2} \rfloor}\right)$, so their squared minimum toroidal distance to each other is

$$2 \cdot \left(2^{\lfloor \frac{m}{2} \rfloor}\right)^2 = 2^m.$$

The squared distance between the diagonals with slope 1 is

$$2 \cdot \left(\frac{2^{\lceil \frac{m}{2} \rceil}}{2}\right)^2 = 2^m.$$

In conclusion, the minimum toroidal distance is $\sqrt{2^m}$. As the diagonals can be tiled seamlessly, the result is identical for the toroidal distance measure. On the unit square $[0,1)^2$, we need to divide the point coordinates by 2^m, so the minimum toroidal distance on the unit square is $\frac{\sqrt{2^m}}{2^m} = \sqrt{2^{-m}}$, which concludes the proof. □

The theorem allows for an additional interpretation of the structure: Using Equation (4), we can solve for d and w given $u_{d,w}$:

$$\begin{aligned} d &= u_{d,w} \bmod 2^{\lfloor \frac{m}{2} \rfloor}, \\ w &= \frac{(u_{d,w} - 2^m \phi_2(d) - d) \bmod 2^m}{2^{\lfloor \frac{m}{2} \rfloor}}. \end{aligned}$$

Inserting these equations into Equation (5) yields

$$\begin{aligned} v_{d,w} &= d + \left(u_{d,w} - 2^m \phi_2\left(u_{d,w} \bmod 2^{\lfloor \frac{m}{2} \rfloor}\right) - d\right) \bmod 2^m \\ &= \left(u_{d,w} - 2^m \phi_2\left(u_{d,w} \bmod 2^{\lfloor \frac{m}{2} \rfloor}\right)\right) \bmod 2^m, \end{aligned} \tag{7}$$

which can be regarded as replicating a $(0, \lfloor \frac{m}{2} \rfloor, 2)$ integer Hammersley-net $2^{\lceil \frac{m}{2} \rceil}$ times horizontally, scaling each one vertically by $-2^{\lceil \frac{m}{2} \rceil}$ and finally adding a linear component to the combination of nets. The resulting points are wrapped around the unit square.

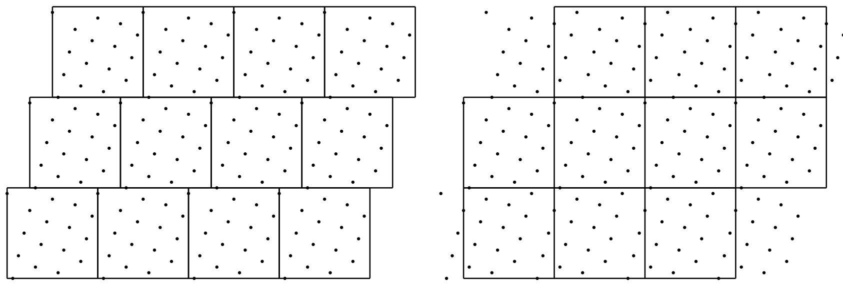


Fig. 6 On the left, the modified tiling for the permutation construction is shown: m is even and each row of the tiling is shifted by $(2^{m-2}, 0)$ relative to its adjacent row below. Using an axis aligned tiling on the right reveals that all tiles in a row share the same sample pattern, while the pattern differs by row by a modulo wrap-around in direction of the x-axis.

3.2.2 Construction for Even m

For even $m \leq 6$ the permutation search did not reveal an improvement of the minimum toroidal distance in comparison to the full matrix search. We would like to note that the permutation search for $m = 6$ did not finish, though. However, when allowing a distance measure that accounts for a slightly irregular tiling, an approach very much resembling the previous construction can be taken, yielding the nets shown in Figure 3.

Using a tiling where each row is shifted by $(2^{m-2}, 0)$ relative to its adjacent row below (see Figure 6), we can get a seamless tiling using $2^{\frac{m}{2}}$ diagonals, each with $2^{\frac{m}{2}}$ points. Again, the points are spaced evenly on each diagonal, this time by the offset vector $(2^{\frac{m}{2}-2}, 2^{\frac{m}{2}})$. The position of the point with the smallest second coordinate on the d-th diagonal, where $d \in \left\{0, \ldots, 2^{\frac{m}{2}} - 1\right\}$, is given by $(2^m \phi_2(d) + \left\lfloor \frac{d}{4} \right\rfloor + 2^{\frac{m}{2}-2}, d)$. With the modified tiling described above, these diagonals are continued seamlessly.

These nets cannot be generated via the classical way of using generator matrices as the point $(0, 0)$ is not included.

While we believe that a similar proof that $t = 0$ is possible as for the odd m case, we only verified the $t = 0$ property using a computer program for all even $m \leq 22$. The minimum toroidal distance equals $\sqrt{241}$ for $m = 8$ and $\sqrt{241 \cdot 2^{m-8}}/2^m$ for all even m where $10 \leq m \leq 22$. See Table 1 for minimum toroidal distance values for $m < 8$. We would like to stress that the modified minimum toroidal distance measure that respects the shifts of the rows in the tiling has been used for these measurements.

Considering a superimposed axis-aligned tiling as illustrated in Figure 6 reveals that in a row each tile contains the same set of samples, while the set of samples varies by row. This in turn allows for constructing a larger pattern that consists of shifted copies of the original pattern as shown in Figure 7. Four rows and four columns of such modulo-wrapped patterns were combined

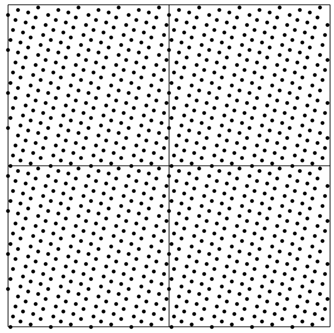


Fig. 7 By taking 4×4 modulo-wrapped copies of the same pattern (see Figure 6), we obtain a larger pattern that is periodic and matches the pixel arrangement. It can be tiled regularly without a decrease in minimum toroidal distance.

to generate a larger pattern. This pattern can be tiled regularly without a decrease in minimum toroidal distance.

3.3 Implementation for General m

Exploiting the fact that we are generating nets in base 2, all operations needed to implement the permutation net constructions described above can be implemented very efficiently without any multiplications. A small `C++` class that generates the point sets directly for even and odd $m \geq 4$ is available at `http://gruenschloss.org/diag0m2/gendiag0m2.h`. In terms of performance, it is comparable to the generation of rank-1 lattice points and also includes code to generate points with the modified tiling explained above.

As an example, we would like to show the implementation of Equation (7). Given the function `phi2` to compute the van der Corput radical inverse in base 2 [9], the implementation `y` has a one line body.

```
inline unsigned int phi2(unsigned int bits) { // for 32 bits
  bits = (bits << 16) | (bits >> 16);
  bits = ((bits & 0x00ff00ff) << 8) | ((bits & 0xff00ff00) >> 8);
  bits = ((bits & 0x0f0f0f0f) << 4) | ((bits & 0xf0f0f0f0) >> 4);
  bits = ((bits & 0x33333333) << 2) | ((bits & 0xcccccccc) >> 2);
  bits = ((bits & 0x55555555) << 1) | ((bits & 0xaaaaaaaa) >> 1);
  return bits;
}

inline unsigned int y(const unsigned int x, const unsigned int m) {
  return (x - (phi2(x & ~-(1 << (m >> 1))) >> (32 - m))) & ~-(1U << m);
}
```

For successive point requests this can be optimized by precomputing the bitmasks and the $2^{\lfloor \frac{m}{2} \rfloor}$ different radical inverse values.

4 Conclusion

We constructed new $(0, m, s)$-nets in base 2 for $s = 2, 3$, which are constrained by maximizing the minimum toroidal distance. Especially the $(0, m, 3)$-net has many applications in computer graphics such as computing anti-aliasing and motion blur in the Reyes architecture [1].

Acknowledgements We would like to thank the reviewers and editors for their very helpful comments. We would also like to thank Sabrina Dammertz, Johannes Hanika, Sehera Nawaz, Matthias Raab, and Daniel Seibert for helpful discussions.

References

1. Cook, R., Carpenter, L., Catmull, E.: The Reyes image rendering architecture. SIGGRAPH Computer Graphics **21**(4), 95–102 (1987)
2. Dammertz, S., Keller, A.: Image synthesis by rank-1 lattices. In: A. Keller, S. Heinrich, H. Niederreiter (eds.) Monte Carlo and Quasi-Monte Carlo Methods 2006, pp. 217–236. Springer (2008)
3. Faure, H.: Discrépance de suites associées à un système de numération (en dimension s). Acta Arithmetica **41**(4), 337–351 (1982)
4. Faure, H.: Discrepancy and diaphony of digital $(0, 1)$-sequences in prime base. Acta Arithmetica **117**, 125–148 (2005)
5. Faure, H., Tezuka, S.: Another random scrambling of digital (t, s)-sequences. In: K. Fang, F. Hickernell, H. Niederreiter (eds.) Monte Carlo and Quasi-Monte Carlo Methods 2000, pp. 242–256. Springer-Verlag, Berlin (2002)
6. Grünschloß, L., Hanika, J., Schwede, R., Keller, A.: (t, m, s)-nets and maximized minimum distance. In: A. Keller, S. Heinrich, H. Niederreiter (eds.) Monte Carlo and Quasi-Monte Carlo Methods 2006, pp. 397–412. Springer (2008)
7. Hofer, R., Larcher, G.: On existence and discrepancy of certain digital Niederreiter-Halton sequences (2009). To appear in Acta Arithmetica
8. Keller, A.: Myths of computer graphics. In: H. Niederreiter (ed.) Monte Carlo and Quasi-Monte Carlo Methods 2004, pp. 217–243. Springer (2006)
9. Kollig, T., Keller, A.: Efficient multidimensional sampling. Computer Graphics Forum **21**(3), 557–563 (2002)
10. Larcher, G., Pillichshammer, F.: Walsh series analysis of the L_2-discrepancy of symmetrisized point sets. Monatsheft Mathematik **132**, 1–18 (2001)
11. Larcher, G., Pillichshammer, F.: Sums of distances to the nearest integer and the discrepancy of digital nets. Acta Arithmetica **106**, 379–408 (2003)
12. Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods. SIAM, Philadelphia (1992)
13. Pharr, M., Humphreys, G.: Physically Based Rendering: From Theory to Implementation. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (2004)
14. Sedgewick, R.: Permutation generation methods. ACM Computing Surveys **9**(2), 137–164 (1977)
15. Sobol', I.: On the distribution of points in a cube and the approximate evaluation of integrals. Zhurnal Vychislitelnoi Matematiki i Matematicheskoi Fiziki **7**(4), 784–802 (1967)