On the mean square weighted $\mathcal{L}_2$ discrepancy of randomized digital nets in prime base

Ligia L. Cristea [a,1], Josef Dick [b,2], Friedrich Pillichshammer [a,*,1]

[a] *Institut für Finanzmathematik, Universität Linz, Altenbergerstraße 69, A-4040 Linz, Austria*

[b] *School of Mathematics, University of New South Wales, Sydney 2052, Australia*

Abstract

We study the mean square weighted $\mathcal{L}_2$ discrepancy of randomized digital (t, m, s)-nets over $\mathbb{Z}_p$. The randomization method considered here is a digital shift of depth m, i.e., for each coordinate the first m digits of each point are shifted by the same shift whereas the remaining digits in each coordinate are shifted independently for each point. We also consider a simplified version of this shift.

We give a formula for the mean square weighted $\mathcal{L}_2$ discrepancy using the generating matrices of the digital net and we prove an upper bound on this discrepancy. Further we investigate how the constant of the leading term depends on the choice of the base p.

Key words: QMC algorithm, randomized digital net, weighted $\mathcal{L}_2$ discrepancy.
1991 MSC: 11K38, 11K06

[*] Corresponding author
Email addresses: ligia-loretta.cristea@jku.at (Ligia L. Cristea), josi@maths.unsw.edu.au (Josef Dick), friedrich.pillichshammer@jku.at (Friedrich Pillichshammer).

[1] Supported by the Austrian Research Foundation (FWF), Project S9609, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

[2] Supported by the Australian Research Council under its Center of Excellence Program.

1 Introduction

In order to compute a multidimensional integral $I(f) = \int_{[0,1]^s} f(\boldsymbol{x}) \mathrm{d}\boldsymbol{x}$ one often uses the mean of function evaluations

$$Q(f) = \frac{1}{N} \sum_{\boldsymbol{x} \in P} f(\boldsymbol{x})$$

as an approximation for $I(f)$. Here P is some random or deterministic sample of N points in the s-dimensional unit cube $[0,1]^s$. The integration rule $Q(f)$ is often called a Monte Carlo (MC) or a quasi-Monte Carlo (QMC) algorithm, depending on whether the sample points P are chosen randomly or deterministically. Many integration error bounds take the form

$$|I(f) - Q(f)| \leq V(f) D(P), \tag{1}$$

where $V(f)$ is a measure for the variation of the integrand f and $D(P)$ is a measure for the non-uniformity for the sample points P. (For example in the classical Koksma-Hlawka inequality $V(f)$ is the variation of f in the sense of Hardy and Krause and $D(P)$ is the star discrepancy of the point set P, see [5,6,12].)

One very popular measure for the non-uniformity of point sets in the unit cube is the so-called $\mathcal{L}_2$ discrepancy which is in the classical case the $\mathcal{L}_2$ norm of the discrepancy function. Nowadays many error bounds (1) use generalizations of this classical case. In this paper we consider the weighted $\mathcal{L}_2$ discrepancy. This discrepancy was introduced by Sloan and Woźniakowski [18] with the aim to give an error estimate of the form (1) which takes imbalances in the "importance" of the projections of the integrand into account. Before we give the definition of the weighted $\mathcal{L}_2$ discrepancy we have to introduce some notation.

Let D denote the index set $D = \{1, \ldots, s\}$. For $\mathfrak{u} \subseteq D$ let $\gamma_{\mathfrak{u}}$ be a non-negative real number, $|\mathfrak{u}|$ the cardinality of $\mathfrak{u}$ and for a vector $\boldsymbol{x} \in [0,1)^s$ let $\boldsymbol{x}_{\mathfrak{u}}$ denote the vector from $[0,1)^{|\mathfrak{u}|}$ containing all components of $\boldsymbol{x}$ whose indices are in $\mathfrak{u}$. Further let $\mathrm{d}\boldsymbol{x}_{\mathfrak{u}} = \prod_{j \in \mathfrak{u}} \mathrm{d}x_j$ and let $(\boldsymbol{x}_{\mathfrak{u}}, 1)$ be the vector from $[0,1)^s$ with all components whose indices are not in $\mathfrak{u}$ replaced by 1. For any N points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}$ in $[0,1)^s$ and any $\boldsymbol{z} = (z_1, \ldots, z_s)$ in $[0,1]^s$ let

$$\mathrm{disc}(\boldsymbol{z}) := \frac{\#\{i : \boldsymbol{x}_i \in [0, \boldsymbol{z})\}}{N} - z_1 \cdots z_s.$$

Then the weighted $\mathcal{L}_2$ discrepancy $\mathcal{L}_{2,N,\boldsymbol{\gamma}}$ of the point set $P_N = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$

is defined as (see [18])

$$\mathcal{L}_{2,N,\gamma}(P_N)=\left(\sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\int_{[0,1]^{|\mathfrak{u}|}}\mathrm{disc}((\boldsymbol{x}_{\mathfrak{u}},1))^2\mathrm{d}\boldsymbol{x}_{\mathfrak{u}}\right)^{1/2}. \qquad (2)$$

Note that for $\gamma_D=1$ and $\gamma_{\mathfrak{u}}=0$ for all $\mathfrak{u}\subset D$ we obtain the classical $\mathcal{L}_2$ discrepancy. The weighted $\mathcal{L}_2$ discrepancy is intimately related to the worst case error of multivariate integration in weighted Sobolev spaces of functions on $[0,1]^s$. For more information in this direction we refer to the paper of Sloan and Woźniakowski [18].

There is a well known formula for the classical $\mathcal{L}_2$ discrepancy due to Warnock [20], which can easily be generalized to obtain a formula for the weighted $\mathcal{L}_2$ discrepancy (see [9] or [10]).

Proposition 1 *Let $P_N=\{\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{N-1}\}$ be a point set in $[0,1)^s$. Then we have*

$$\mathcal{L}^2_{2,N,\gamma}(P_N)=$$
$$\sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\left[\frac{1}{3^{|\mathfrak{u}|}}-\frac{2}{N}\sum_{n=0}^{N-1}\prod_{j\in\mathfrak{u}}\frac{1-x_{n,j}^2}{2}+\frac{1}{N^2}\sum_{n,h=0}^{N-1}\prod_{j\in\mathfrak{u}}\min(1-x_{n,j},1-x_{h,j})\right],$$

where $x_{n,j}$ is the j-th component of the point $\boldsymbol{x}_n$.

Currently the most effective constructions of point sets with good equidistribution properties are based on the concept of (t,m,s)-nets in a base b, see [11,12]. In practise all concrete constructions of (t,m,s)-nets in a base b are based on a general construction scheme which is the concept of digital nets, see [7,8,11,12]. See also [13] for a very recent survey article. Here in this paper we only deal with the case where $b=p$ is a prime number. In the following let $\mathbb{Z}_p$ denote the finite field with p elements, $p\geq 2$ a prime number.

Definition 1 Let $s\geq 1$, $m\geq 1$ and $0\leq t\leq m$ be integers. Choose s $m\times m$ matrices $C_1,\ldots,C_s$ over $\mathbb{Z}_p$ with the following property: for any integers $d_1,\ldots,d_s\geq 0$ with $d_1+\cdots+d_s=m-t$ the system of the

first d_1 rows of C_1, together with the
$\vdots$
first d_{s-1} rows of C_{s-1}, together with the
first d_s rows of C_s

is linearly independent over $\mathbb{Z}_p$. Consider the following construction principle for point sets consisting of p^m points in $[0,1)^s$: represent n, $0\leq n<p^m$, in

base p, $n = n_0 + n_1 p + \cdots + n_{m-1} p^{m-1}$, and multiply the matrix C_j, $1 \leq j \leq s$, with the vector $\vec{n} = (n_0, \ldots, n_{m-1})^\top$ of digits of n in $\mathbb{Z}_p$,

$$C_j \vec{n} =: (y_1^{(j)}(n), \ldots, y_m^{(j)}(n))^\top \in \mathbb{Z}_p^m.$$

Now we set

$$x_n^{(j)} := \frac{y_1^{(j)}(n)}{p} + \cdots + \frac{y_m^{(j)}(n)}{p^m} \qquad \text{and} \qquad \boldsymbol{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}).$$

The point set $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{p^m-1}\}$ is called a digital (t, m, s)-net over $\mathbb{Z}_p$ and the matrices $C_1, \ldots, C_s$ are called the generating matrices of the digital net.

The quality of a (digital) (t, m, s)-net is expressed by the so-called quality parameter $t \in \{0, 1, \ldots, m\}$. Small values of t imply strong distribution properties of the net. However, the optimal value $t = 0$ is not possible for arbitrary choices of m, p and s. Note that it follows from Definition 1 that any d-dimensional projection, $1 \leq d \leq s$, of a digital (t, m, s)-net over $\mathbb{Z}_p$ is a digital (t, m, d)-net over $\mathbb{Z}_p$.

For practical applications it is often useful to have a random element in the point set used (see [10]). On the other hand we wish to preserve the structure and distribution properties which a point set already has. That is in this case, we wish to randomize a (t, m, s)-net such that the resulting point set is again a (t, m, s)-net with the same quality parameter t. Several randomization methods for (t, m, s)-nets have been introduced (see [10,14,21]). The randomization method considered in this paper is a digital shift of depth m (see also [4,10]) and a simplified version of such a shift which is more useful for practical applications. Previously, the expected value of the weighted $\mathcal{L}_2$ discrepancy of digitally shifted digital (t, m, s)-nets over $\mathbb{Z}_2$ has been analyzed in [4].

The aim of this paper is to generalize the results from [4] to digital nets over $\mathbb{Z}_p$, where p is a prime number and to show that similar results hold for the simplified digital shift. We succeed in generalizing the formula for the mean square weighted $\mathcal{L}_2$ discrepancy in [4] to arbitrary prime bases p (see Theorem 1) and to show that an analogous formula holds for the simplified version of a shift of depth m. We then use these results to obtain an upper bound on the mean square weighted $\mathcal{L}_2$ discrepancy (see Theorem 2). Note that by a lower bound on the $\mathcal{L}_2$ discrepancy of Roth [17] it follows that the $\mathcal{L}_2$ discrepancy of any point set in the s dimensional unit cube must be at least of order $(\log N)^{(s-1)/2} N^{-1}$, where N is the number of points. As in [4] we also obtain this convergence rate for digital (t, m, s)-nets over $\mathbb{Z}_p$. On the other hand we are also interested in how the constant $A(p)$ of the leading term, that is,

$$A(p) := \limsup_{m\to\infty} \frac{p^m \sqrt{\mathbb{E}(|\mathcal{L}^2_{2,p^m}(P_{p^m})|)}}{(\log p^m)^{(s-1)/2}} \tag{3}$$

behaves for various choices of p. This is investigated in Section 4. It is generally believed that using $p = 2$ yields the best results. This is also verified by our calculations here. In particular we consider the Hammersley net. In this special case we are able to calculate $A(p)$ exactly which shows that the constant in the leading term is of order $O(p(\log p)^{-1/2})$ and hence we obtain the smallest constant when $p = 2$. For the general case we can only obtain an upper bound, again with the constant of the leading term growing in p and with the smallest value obtained for $p = 2$. On the other hand it is conceivable that smaller constants can be obtained using digital nets with higher bases, but until now no such bound has been proven.

In the following we introduce the digital shift of depth m for the one dimensional case. For higher dimensions each coordinate is randomized independently and therefore one just needs to apply the one dimensional randomization method to each coordinate independently.

Let the point set $P_{p^m} = \{x_0, \ldots, x_{p^m-1}\}$ be a digital $(t, m, 1)$-net over $\mathbb{Z}_p$ generated by the matrix C. Let

$$x_n = \frac{x_{n,1}}{p} + \frac{x_{n,2}}{p^2} + \cdots + \frac{x_{n,m}}{p^m}$$

be the p-adic digit expansion of x_n.

Now we choose the digits $\sigma_1, \ldots, \sigma_m \in \{0, 1, \ldots, p-1\}$ i.i.d.. Then we define

$$z_{n,i} \equiv x_{n,i} + \sigma_i \pmod{p} \qquad \text{for } i = 1, \ldots, m$$

with $z_{n,i} \in \{0, 1, \ldots, p-1\}$. Further, for $n = 0, \ldots, p^m - 1$, we choose $\delta_n \in [0, \frac{1}{p^m})$ i.i.d.. Then the randomized point set $\widetilde{P}_{p^m} = \{z_0, \ldots, z_{p^m-1}\}$ is given by

$$z_n = \frac{z_{n,1}}{p} + \cdots + \frac{z_{n,m}}{p^m} + \delta_n.$$

This means that we apply the same digital shift to the first m digits, whereas the following digits are shifted independently for each x_n. Therefore we call it a digital shift of depth m (see again [10]).

Sometimes we will write digital shift or simply shift instead of digital shift of depth m. When we use a digital shift of depth m' in conjunction with digital (t, m, s)-nets we always assume that $m' = m$.

Further we introduce the simplified version of a digital shift of depth m. With the notations from above the randomized point set $\widehat{P}_{p^m} = \{z_0, \ldots, z_{p^m-1}\}$ is given by

$$z_n = \frac{z_{n,1}}{p} + \cdots + \frac{z_{n,m}}{p^m} + \frac{1}{2p^m}.$$

This means we apply the same digital shift to the first m digits and then we add to each point the quantity $1/(2p^m)$. Geometrically this means that the randomized points are no longer on the left boundary of intervals $[a/p^m, (a+1)/p^m)$ but they are moved to the midpoints of such intervals. Note that for the simplified digital shift we only have p^m possibilities which means a very strong de-randomization compared to the shift of depth m.

For arbitrary $s \geq 1$ it can be shown that a (t, m, s)-net in base p randomized by a digital shift of depth m or a simplified digital shift independently in each coordinate is again a (t, m, s)-net in base p with the same quality parameter t. As the result is not essential for the following we omit the proof. Similar results have been shown before (see for example [3,14]).

2 Walsh functions and their connection to digital nets

In this section we recall the definition of Walsh functions, which will be the main tool in our analysis of the mean square weighted $\mathcal{L}_2$ discrepancy. We confine ourselves to prime-base p. In the following let $\mathbb{N}_0$ denote the set of non-negative integers and $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ the unit circle in the complex plane.

Definition 2 For a non-negative integer k with base p representation

$$k = \kappa_{a-1} p^{a-1} + \cdots + \kappa_1 p + \kappa_0,$$

with $\kappa_i \in \{0, 1, \ldots, p-1\}$, we define the Walsh function ${}_p\mathrm{wal}_k : [0,1) \longrightarrow \mathbb{T}$ by

$${}_p\mathrm{wal}_k(x) := \mathrm{e}^{\frac{2\pi \mathrm{i}}{p}(x_1\kappa_0 + \cdots + x_a\kappa_{a-1})},$$

for $x \in [0,1)$ with base p representation $x = \frac{x_1}{p} + \frac{x_2}{p^2} + \cdots$ (unique in the sense that infinitely many of the x_i must be different from $p-1$).

Definition 3 For dimension $s \geq 2$, $x_1, \ldots, x_s \in [0,1)$ and $k_1, \ldots, k_s \in \mathbb{N}_0$ we define ${}_p\mathrm{wal}_{k_1,\ldots,k_s} : [0,1)^s \longrightarrow \mathbb{T}$ by

$${}_p\mathrm{wal}_{k_1,\ldots,k_s}(x_1, \ldots, x_s) := \prod_{j=1}^{s} {}_p\mathrm{wal}_{k_j}(x_j).$$

For vectors $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$ and $\boldsymbol{x} = (x_1, \ldots, x_s) \in [0,1)^s$ we write

$${}_p\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}) :=_p \mathrm{wal}_{k_1,\ldots,k_s}(x_1, \ldots, x_s).$$

Throughout the paper we will use Walsh functions in base p, hence we shall often write wal instead of ${}_p\mathrm{wal}$.

We introduce some notations. By $\oplus$ we denote the digit-wise addition modulo p and by $\ominus$ the digit-wise subtraction modulo p , i.e., for $x = \sum_{i=w}^{\infty} \frac{x_i}{p^i}$ and $y = \sum_{i=w}^{\infty} \frac{y_i}{p^i}$ for some integer w we have

$$x \oplus y := \sum_{i=w}^{\infty} \frac{z_i}{p^i}, \quad \text{where} \quad z_i \equiv x_i + y_i \,(\mathrm{mod}\ p),$$

$$x \ominus y := \sum_{i=w}^{\infty} \frac{z_i}{p^i}, \quad \text{where} \quad z_i \equiv x_i - y_i \,(\mathrm{mod}\ p).$$

Correspondingly we define $\ominus y := \sum_{i=w}^{\infty} \frac{z_i}{p^i}$, where $z_i \equiv -y_i \,(\mathrm{mod}\ p)$.

In the following proposition we summarize some basic properties of Walsh functions. For more information see [2,15,16,19].

Proposition 2 *(1) For all $k, l \in \mathbb{N}_0$ and all $x, y \in [0,1)$, with the restriction that if x, y are not p-adic rationals then $x \oplus y$ is not allowed to be a p-adic rational, we have*

$$wal_k(x) \cdot wal_l(x) = wal_{k \oplus l}(x), \quad wal_k(x) \cdot wal_k(y) = wal_k(x \oplus y),$$

$$wal_k(x) \cdot \overline{wal_l(x)} = wal_{k \ominus l}(x), \quad wal_k(x) \cdot \overline{wal_k(y)} = wal_k(x \ominus y).$$

(2) We have

$$\int_0^1 wal_0(x) \mathrm{d}x = 1 \quad \textit{and} \quad \int_0^1 wal_k(x) \mathrm{d}x = 0 \ \textit{if}\ k > 0.$$

(3) For all $\boldsymbol{k}, \boldsymbol{l} \in \mathbb{N}_0^s$ we have the following orthogonality properties:

$$\int_{[0,1]^s} wal_{\boldsymbol{k}}(\boldsymbol{x}) \overline{wal_{\boldsymbol{l}}(\boldsymbol{x})} \mathrm{d}\boldsymbol{x} = \begin{cases} 1 & \textit{if } \boldsymbol{k} = \boldsymbol{l}, \\ 0 & \textit{otherwise.} \end{cases}$$

(4) For any $f \in \mathcal{L}_2([0,1)^s)$ and any $\boldsymbol{\sigma} \in [0,1)^s$ we have

$$\int_{[0,1]^s} f(\boldsymbol{x}) \mathrm{d}\boldsymbol{x} = \int_{[0,1]^s} f(\boldsymbol{x} \oplus \boldsymbol{\sigma}) \mathrm{d}\boldsymbol{x}.$$

(5) For any integer $s \geq 1$ the system $\{wal_{k_1,\ldots,k_s} : k_1, \ldots, k_s \geq 0\}$ is a complete orthonormal system in $\mathcal{L}_2([0,1]^s)$.

Proof. The proofs of (1)-(3) are straightforward, or see [15]. For item (4) see [2, Lemma 1] or [15, Corollary 4] and for item (5) see [2] or [15, Satz 1]. □

Let $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{p^m-1}\}$ be a digital net over $\mathbb{Z}_p$ generated by the $m \times m$ matrices $C_1, \ldots, C_s$ over $\mathbb{Z}_p$. For $\boldsymbol{x}_n = (x_{n,1}, \ldots, x_{n,s})$ and $x_{n,j} = \frac{x_{n,j,1}}{p} + \cdots + \frac{x_{n,j,m}}{p^m}$, $1 \le j \le s$, $0 \le n < p^m$, we identify $\boldsymbol{x}_n$ with

$$(x_{n,1,1}, \ldots, x_{n,1,m}, \ldots, x_{n,s,1}, \ldots, x_{n,s,m}) \in \mathbb{Z}_p^{ms}$$

and define

$$\boldsymbol{x}_n \oplus \boldsymbol{x}_h := (x_{n,1,1} + x_{h,1,1}, \ldots, x_{n,s,m} + x_{h,s,m}) \in \mathbb{Z}_p^{ms}. \tag{4}$$

The subsequent lemma follows easily from the construction of digital nets.

Lemma 1 *Any digital net $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{p^m-1}\}$ over $\mathbb{Z}_p$ is a subgroup of $(\mathbb{Z}_p^{ms}, \oplus)$.*

The following lemma will be very useful for our investigation.

Lemma 2 *Let $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{p^m-1}\}$ be a digital (t, m, s)-net over $\mathbb{Z}_p$ generated by the $m \times m$ matrices $C_1, \ldots, C_s$ over $\mathbb{Z}_p$. Then for all integers $0 \le k_1, \ldots, k_s < p^m$ we have*

$$\sum_{n=0}^{p^m-1} wal_{k_1,\ldots,k_s}(\boldsymbol{x}_n) = \begin{cases} p^m & \textit{if } C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s = \vec{0}, \\ 0 & \textit{otherwise,} \end{cases}$$

where for $0 \le k < p^m$ with $k = \kappa_0 + \kappa_1 p + \cdots + \kappa_{m-1} p^{m-1}$ we write $\vec{k} = (\kappa_0, \ldots, \kappa_{m-1})^\top \in \mathbb{Z}_p^m$ and $\vec{0}$ denotes the zero vector in $\mathbb{Z}_p^m$.

Proof. See [3, Lemma 2]. □

3 On the mean square weighted $\mathcal{L}_2$ discrepancy of randomized nets

In the following subsection we prove a formula for the mean square weighted $\mathcal{L}_2$ discrepancy of randomized digital nets. This formula depends on the generating matrices of the digital net. We remark that it is possible to prove a similar formula for more general $\mathcal{L}_2$ discrepancies as for example the weighted anchored $\mathcal{L}_2$ discrepancy with anchor $\boldsymbol{c} \in [0,1]^s$. But for simplicity we restrict ourselves to the case $\boldsymbol{c} = (1, \ldots, 1)$ here.

3.1 A formula for the mean square weighted $\mathcal{L}_2$ discrepancy of randomized nets

The aim of this subsection is to prove the following theorem.

Theorem 1 *Let P_{p^m} be a digital (t,m,s)-net over $\mathbb{Z}_p$ with generating matrices $C_1,\ldots,C_s$.*

(i) Let $\widetilde{P}_{p^m}$ be the point set obtained after applying an i.i.d. random digital shift of depth m independently to each coordinate of each point of P_{p^m}. Then the mean square weighted $\mathcal{L}_2$ discrepancy of $\widetilde{P}_{p^m}$ is given by

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m})] = \\ \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \left[\frac{1}{p^m\cdot 2^{|\mathfrak{u}|}}\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right)+\frac{1}{3^{|\mathfrak{u}|}}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\ \mathfrak{v}\neq\emptyset}}\left(\frac{3}{2}\right)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})\right],$$

where for $\mathfrak{v}=\{v_1,\ldots,v_e\}$ we have

$$\mathcal{B}(\mathfrak{v}) = \sum_{\substack{k_1,\ldots,k_e=1\\ C_{v_1}^\top\vec{k}_1+\cdots+C_{v_e}^\top\vec{k}_e=\vec{0}}}^{p^m-1}\prod_{j=1}^{e}\psi(k_j),$$

with

$$\psi(k) = -\frac{1}{p^{2(r+1)}}\left(\frac{1}{3}-\frac{1}{\sin^2(\kappa_r\pi/p)}\right)$$

and $r=r(k)$ is such that $p^{r(k)}\leq k<p^{r(k)+1}$ and κ_r is the most significant bit in the p-adic representation of k.

(ii) Let $\widehat{P}_{p^m}$ be the point set obtained after applying a simplified i.i.d. random digital shift independently to each coordinate of each point of P_{p^m}. Then the mean square weighted $\mathcal{L}_2$ discrepancy of $\widehat{P}_{p^m}$ is given by

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widehat{P}_{p^m})] = \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \left[2\left(\frac{1}{3^{|\mathfrak{u}|}}-\left(\frac{1}{3}+\frac{1}{24\cdot p^{2m}}\right)^{|\mathfrak{u}|}\right)\right. \\ \left.+\frac{1}{p^m\cdot 2^{|\mathfrak{u}|}}\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right)+\frac{1}{3^{|\mathfrak{u}|}}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\ \mathfrak{v}\neq\emptyset}}\left(\frac{3}{2}\right)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})\right],$$

where $\mathcal{B}(\mathfrak{v})$ is as in (i).

From this theorem we immediately obtain

Corollary 1 *Let P_{p^m} be a digital (t,m,s)-net over $\mathbb{Z}_p$. Let $\widetilde{P}_{p^m}$ be the point set obtained after applying an i.i.d. random digital shift of depth m independently to each coordinate of each point of P_{p^m} and let $\widehat{P}_{p^m}$ be the point set obtained after applying an simplified i.i.d. random digital shift independently to each coordinate of each point of P_{p^m}. Then we have*

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widehat{P}_{p^m})] \leq \mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m})].$$

The proof of Theorem 1 is based on the Walsh series representation of the formula for the $\mathcal{L}_2$ discrepancy given in Proposition 1. As we shall see later, the function ψ in the theorem above is related to Walsh coefficients of a certain function appearing in the formula for the $\mathcal{L}_2$ discrepancy. We need several lemmas.

Lemma 3 *Let $x_1, x_2 \in [0,1)$ and let $z_1, z_2 \in [0,1)$ be the points obtained after applying an i.i.d. random digital shift of depth m to x_1 and x_2. Then we have*

$$\mathbb{E}[wal_k(z_1)\overline{wal_l(z_2)}] = \begin{cases} wal_k(x_1 \ominus x_2) & \text{if } 0 \le k = l < p^m, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The proof follows exactly the lines of the proof of [4, Lemma 3] with the dyadic expansions replaced by p-adic expansions. □

In the following lemma we calculate Walsh coefficients of the function $|z_1 - z_2|$. This function appears in the formula for the $\mathcal{L}_2$ discrepancy through the equation $\min(z_1, z_2) = \frac{1}{2}(z_1 + z_2 - |z_1 - z_2|)$.

Lemma 4 *Let $z_1, z_2 \in [0,1)$. We have*

$$|z_1 - z_2| = \sum_{k,l=0}^{\infty} \tau(k,l) wal_k(z_1)\overline{wal_l(z_2)},$$

where $\tau(0) := \tau(0,0) = \frac{1}{3}$ and $\tau(k) := \tau(k,k) = \frac{1}{p^{2(r+1)}}\left(\frac{1}{3} - \frac{1}{\sin^2(\kappa_r \pi/p)}\right)$ for $k > 0$. For $k > 0$, $r(k)$ denotes the unique integer r such that $p^r \le k < p^{r+1}$.

Proof. As $|z_1 - z_2| \in \mathcal{L}_2([0,1]^2)$ it follows from Proposition 2 that the function $|z_1 - z_2|$ can be represented by its Walsh series. We have

$$\tau(k,l) = \int_0^1 \int_0^1 |z_1 - z_2| \overline{\mathrm{wal}_k(z_1)} \mathrm{wal}_l(z_2) \mathrm{d}z_1 \mathrm{d}z_2.$$

For the evaluation of this integral for $k = l$ see [3, Appendix A]. □

Lemma 5 *Let $x_1, x_2 \in [0,1)$ and let $z_1, z_2 \in [0,1)$ be the points obtained after applying an i.i.d. random digital shift of depth m to x_1 and x_2.*

(1) We have

$$\mathbb{E}[z_1] = \frac{1}{2} \quad \text{and} \quad \mathbb{E}[z_1^2] = \frac{1}{3}.$$

(2) We have

$$\mathbb{E}[|z_1 - z_2|] = \sum_{k=0}^{p^m - 1} \tau(k) wal_k(x_1 \ominus x_2),$$

where $\tau(0) = \frac{1}{3}$ and $\tau(k) = \frac{1}{p^{2(r+1)}}\left(\frac{1}{3} - \frac{1}{\sin^2(\kappa_r \pi/p)}\right)$ for $k > 0$. For $k > 0$, $r(k)$ denotes the unique integer r such that $p^r \le k < p^{r+1}$.

(3) We have

$$\mathbb{E}[\min(1-z_1,1-z_2)] = \frac{1}{2}\left(1-\sum_{k=0}^{p^m-1}\tau(k)wal_k(x_1\ominus x_2)\right).$$

Proof. (1) The proof of these two formulae is straightforward.

(2) In Lemma 4 it was shown that

$$|z_1-z_2| = \sum_{k,l=0}^{\infty}\tau(k,l)\mathrm{wal}_k(z_1)\overline{\mathrm{wal}_l(z_2)},$$

where

$$\tau(k)=\tau(k,k)=\frac{1}{p^{2(r+1)}}\left(\frac{1}{3}-\frac{1}{\sin^2(\kappa_r\pi/p)}\right),$$

for $k>0$ and $\tau(0,0)=\frac{1}{3}$. (We do not need to know $\tau(k,l)$ for $k\neq l$ for our purposes here.) The result now follows from the linearity of the expectation value and Lemma 3.

(3) This result follows from items (1) and (2) together with the formula

$$\min(z_1,z_2)=\frac{1}{2}(z_1+z_2-|z_1-z_2|).$$

□

We are now ready to prove Theorem 1.

Proof of Theorem 1. First we prove the formula for the case that the randomization method is the digital shift of depth m. Let $\widetilde{P}_{p^m}=\{\boldsymbol{z}_0,\ldots,\boldsymbol{z}_{p^m-1}\}$ and $\boldsymbol{z}_n=(z_{n,1},\ldots,z_{n,s})$. From Proposition 1, Lemma 5 and the linearity of expectation we get

$$\begin{aligned}\mathbb{E}[\mathcal{L}^2_{2,p^m,\gamma}(\widetilde{P}_{p^m})] =& \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\left[\frac{1}{3^{|\mathfrak{u}|}}-\frac{2}{p^m}\sum_{n=0}^{p^m-1}\prod_{j\in\mathfrak{u}}\frac{1-\mathbb{E}[z_{n,j}^2]}{2}\right.\\ &\left.+\frac{1}{p^{2m}}\sum_{n,h=0}^{p^m-1}\prod_{j\in\mathfrak{u}}\mathbb{E}[\min(1-z_{n,j},1-z_{h,j})]\right]\\ =& \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\left[-\frac{1}{3^{|\mathfrak{u}|}}+\frac{1}{p^{2m}}\sum_{n=0}^{p^m-1}\prod_{j\in\mathfrak{u}}\mathbb{E}[1-z_{n,j}]\right.\\ &\left.+\frac{1}{p^{2m}}\sum_{\substack{n,h=0\\ n\neq h}}^{p^m-1}\prod_{j\in\mathfrak{u}}\mathbb{E}[\min(1-z_{n,j},1-z_{h,j})]\right].\end{aligned}$$

Now we use Lemma 5 again to obtain

$$\begin{aligned}\mathbb{E}[\mathcal{L}^2_{2,p^m,\gamma}(\widetilde{P}_{p^m})] = & \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \Bigg[-\frac{1}{3^{|\mathfrak{u}|}} + \frac{1}{p^m}\frac{1}{2^{|\mathfrak{u}|}} \\ & + \frac{1}{p^{2m}} \sum_{\substack{n,h=0\\ n\neq h}}^{p^m-1} \prod_{j\in\mathfrak{u}} \frac{1}{2}\left(1-\sum_{k=0}^{p^m-1}\tau(k)\mathrm{wal}_k(x_{n,j}\ominus x_{h,j})\right)\Bigg].\end{aligned}$$

We have

$$\begin{aligned}\prod_{j\in\mathfrak{u}}\left(1-\sum_{k=0}^{p^m-1}\tau(k)\mathrm{wal}_k(x_{n,j}\ominus x_{h,j})\right) = 1 + \sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset\\ \mathfrak{w}=\{w_1,\ldots,w_d\}}} (-1)^{|\mathfrak{w}|}\times \\ \sum_{k_1=0}^{p^m-1}\cdots\sum_{k_d=0}^{p^m-1}\tau(k_1)\cdots\tau(k_d)\mathrm{wal}_{k_1,\ldots,k_d}(x_{n,w_1}\ominus x_{h,w_1},\ldots,x_{n,w_d}\ominus x_{h,w_d}).\end{aligned}$$

Thus

$$\begin{aligned}\mathbb{E}[\mathcal{L}^2_{2,p^m,\gamma}(\widetilde{P}_{p^m})] = & \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \Bigg[-\frac{1}{3^{|\mathfrak{u}|}} + \frac{1}{p^m}\frac{1}{2^{|\mathfrak{u}|}} + \frac{1}{p^{2m}}\sum_{\substack{n,h=0\\ n\neq h}}^{p^m-1}\frac{1}{2^{|\mathfrak{u}|}} \\ & + \frac{1}{2^{|\mathfrak{u}|}}\frac{1}{p^{2m}}\sum_{\substack{n,h=0\\ n\neq h}}^{p^m-1}\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset\\ \mathfrak{w}=\{w_1,\ldots,w_d\}}}(-1)^d\times \\ & \sum_{k_1=0}^{p^m-1}\cdots\sum_{k_d=0}^{p^m-1}\prod_{i=1}^{d}\tau(k_i)\mathrm{wal}_{k_i}(x_{n,w_i}\ominus x_{h,w_i})\Bigg].\end{aligned}$$

We have

$$\begin{aligned}\sum_{k=0}^{p^m-1}\tau(k) = & \frac{1}{3} + \sum_{r=0}^{m-1}\sum_{k=p^r}^{p^{r+1}-1}\frac{1}{p^{2(r+1)}}\left(\frac{1}{3}-\frac{1}{\sin^2(\kappa_r\pi/p)}\right) \\ = & \frac{1}{3} + \sum_{r=0}^{m-1}\frac{1}{p^{r+2}}\sum_{a=1}^{p-1}\left(\frac{1}{3}-\frac{1}{\sin^2(a\pi/p)}\right).\end{aligned}$$

We evaluate the second sum in the above expression. In [3, Appendix C] it was shown that

$$\sum_{a=1}^{p-1}\frac{1}{\sin^2(a\pi/p)} = \frac{p^2-1}{3}.$$

Hence we get

$$\sum_{k=0}^{p^m-1}\tau(k) = \frac{1}{3\cdot p^m}.$$

Therefore,

$$\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset}}(-1)^{|\mathfrak{w}|}\sum_{k_1,\ldots,k_{|\mathfrak{w}|}=0}^{p^m-1}\prod_{i=1}^{|\mathfrak{w}|}\tau(k_i)=\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset}}\left(-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{w}|}=\sum_{r=1}^{|\mathfrak{u}|}\binom{|\mathfrak{u}|}{r}\left(-\frac{1}{3\cdot p^m}\right)^r$$
$$=\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}-1.$$

Now we add and substract this in the above expression in order to obtain

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\gamma}(\widetilde{P}_{p^m})]$$
$$=\sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\Bigg[\frac{1}{2^{|\mathfrak{u}|}}-\frac{1}{3^{|\mathfrak{u}|}}+\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right)\frac{1}{p^m}\frac{1}{2^{|\mathfrak{u}|}}$$
$$+\frac{1}{2^{|\mathfrak{u}|}}\frac{1}{p^{2m}}\sum_{n,h=0}^{p^m-1}\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset\\ \mathfrak{w}=\{w_1,\ldots,w_d\}}}(-1)^d\sum_{k_1,\ldots,k_d=0}^{p^m-1}\prod_{i=1}^{d}\tau(k_i)\mathrm{wal}_{k_i}(x_{n,w_i}\ominus x_{h,w_i})\Bigg].$$

Since $\tau(0)=\frac{1}{3}$ we have

$$\frac{1}{p^{2m}}\frac{1}{2^{|\mathfrak{u}|}}\sum_{n,h=0}^{p^m-1}\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset}}(-1)^{|\mathfrak{w}|}\tau(0)^{|\mathfrak{w}|}=\frac{1}{3^{|\mathfrak{u}|}}-\frac{1}{2^{|\mathfrak{u}|}}.$$

Hence

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\gamma}(\widetilde{P}_{p^m})]$$
$$=\sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\Bigg[\frac{1}{2^{|\mathfrak{u}|}}-\frac{1}{3^{|\mathfrak{u}|}}+\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right)\frac{1}{p^m}\frac{1}{2^{|\mathfrak{u}|}}+\frac{1}{3^{|\mathfrak{u}|}}-\frac{1}{2^{|\mathfrak{u}|}}$$
$$+\frac{1}{2^{|\mathfrak{u}|}}\frac{1}{p^{2m}}\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\ \mathfrak{w}\neq\emptyset\\ \mathfrak{w}=\{w_1,\ldots,w_d\}}}(-1)^d\sum_{\substack{k_1,\ldots,k_d=0\\ (k_1,\ldots,k_d)\neq(0,\ldots,0)}}^{p^m-1}\sum_{n,h=0}^{p^m-1}\prod_{i=1}^{d}\tau(k_i)\mathrm{wal}_{k_i}(x_{n,w_i}\ominus x_{h,w_i})\Bigg].$$

From the group structure of digital nets (see Lemma 1) and from Lemma 2 it follows that for any digital net $\{\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{p^m-1}\}$ generated by the $m\times m$ matrices $C_1,\ldots,C_s$, we have

$$\frac{1}{p^{2m}}\sum_{n,h=0}^{p^m-1}\mathrm{wal}_{k_1,\ldots,k_s}(\boldsymbol{x}_n\ominus\boldsymbol{x}_h)=\frac{1}{p^m}\sum_{n=0}^{p^m-1}\mathrm{wal}_{k_1,\ldots,k_s}(\boldsymbol{x}_n)$$
$$=\begin{cases}1 & \text{if } C_1^\top\vec{k}_1+\cdots+C_s^\top\vec{k}_s=\vec{0},\\ 0 & \text{otherwise.}\end{cases}$$

Since we have that the d-dimensional projection of a digital (t,m,s)-net is again a digital (t,m,d)-net (see Introduction) we get (with $\mathfrak{w}=\{w_1,\ldots,w_d\}$)

$$\begin{aligned}
&\sum_{\substack{k_1,\ldots,k_d=0\\(k_1,\ldots,k_d)\neq(0,\ldots,0)}}^{p^m-1}\ \sum_{n,h=0}^{p^m-1}\prod_{j=1}^{d}\tau(k_j)\mathrm{wal}_{k_j}(x_{n,w_j}\ominus x_{h,w_j})\\
&=p^{2m}\sum_{\substack{k_1,\ldots,k_d=0\\(k_1,\ldots,k_d)\neq(0,\ldots,0)\\C_{w_1}^\top\vec{k}_1+\cdots+C_{w_d}^\top\vec{k}_d=\vec{0}}}^{p^m-1}\ \prod_{i=1}^{d}\tau(k_i)\\
&=p^{2m}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{w}\\\mathfrak{v}\neq\emptyset\\\mathfrak{v}=\{v_1,\ldots,v_e\}}}\frac{1}{3^{|\mathfrak{w}|-|\mathfrak{v}|}}\sum_{\substack{k_1,\ldots,k_e=1\\C_{v_1}^\top\vec{k}_1+\cdots+C_{v_e}^\top\vec{k}_e=\vec{0}}}^{p^m-1}\ \prod_{j=1}^{e}\tau(k_j).
\end{aligned}$$

As $\prod_{j=1}^{e}\tau(k_j)=(-1)^e\prod_{j=1}^{e}\psi(k_j)$ we have

$$\sum_{\substack{k_1,\ldots,k_d=0\\(k_1,\ldots,k_d)\neq(0,\ldots,0)}}^{p^m-1}\ \sum_{n,h=0}^{p^m-1}\prod_{j=1}^{d}\tau(k_j)\mathrm{wal}_{k_j}(x_{n,w_j}\ominus x_{h,w_j})=\frac{p^{2m}}{3^{|\mathfrak{w}|}}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{w}\\\mathfrak{v}\neq\emptyset}}(-3)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v}).$$

Thus we obtain

$$\begin{aligned}
\mathbb{E}[\mathcal{L}^2_{2,p^m,\gamma}(\widetilde{P}_{p^m})]=&\sum_{\substack{\mathfrak{u}\subseteq D\\\mathfrak{u}\neq\emptyset}}\gamma_{\mathfrak{u}}\Bigg[\frac{1}{p^m\cdot 2^{|\mathfrak{u}|}}\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right)\\
&+\frac{1}{2^{|\mathfrak{u}|}}\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\\mathfrak{w}\neq\emptyset}}\left(-\frac{1}{3}\right)^{|\mathfrak{w}|}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{w}\\\mathfrak{v}\neq\emptyset}}(-3)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})\Bigg].
\end{aligned}$$

Let now $\mathfrak{u},\mathfrak{v}$, with $\emptyset\neq\mathfrak{v}\subseteq\mathfrak{u}\subseteq D$, be fixed. Then $\mathfrak{v}\subseteq\mathfrak{w}\subseteq\mathfrak{u}$ is equivalent to $(\mathfrak{w}\setminus\mathfrak{v})\subseteq(\mathfrak{u}\setminus\mathfrak{v})$, provided that $\mathfrak{v}\subseteq\mathfrak{w}$. Therefore, for $|\mathfrak{v}|\leq w\leq|\mathfrak{u}|$, there are $\binom{|\mathfrak{u}|-|\mathfrak{v}|}{w-|\mathfrak{v}|}$ sets $\mathfrak{w}$ such that $|\mathfrak{w}|=w$ and $\mathfrak{v}\subseteq\mathfrak{w}\subseteq\mathfrak{u}$. Hence

$$\begin{aligned}
\sum_{\substack{\mathfrak{w}\subseteq\mathfrak{u}\\\mathfrak{w}\neq\emptyset}}\left(-\frac{1}{3}\right)^{|\mathfrak{w}|}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{w}\\\mathfrak{v}\neq\emptyset}}(-3)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})&=\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\\mathfrak{v}\neq\emptyset}}\sum_{w=|\mathfrak{v}|}^{|\mathfrak{u}|}\binom{|\mathfrak{u}|-|\mathfrak{v}|}{w-|\mathfrak{v}|}\left(-\frac{1}{3}\right)^{w}(-3)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})\\
&=\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\\mathfrak{v}\neq\emptyset}}\sum_{w=0}^{|\mathfrak{u}|-|\mathfrak{v}|}\binom{|\mathfrak{u}|-|\mathfrak{v}|}{w}\left(-\frac{1}{3}\right)^{w}\mathcal{B}(\mathfrak{v})\\
&=\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\\mathfrak{v}\neq\emptyset}}\left(\frac{2}{3}\right)^{|\mathfrak{u}|-|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})
\end{aligned}$$

and the first result follows.

It remains to prove the formula for the mean square weighted $\mathcal{L}_2$ discrepancy for the case that the randomization method is a simplified digital shift. Trivially we have

$$p^m \int_0^{1/p^m} [1-(x_{n,j}+\delta_n)]\, \mathrm{d}\delta_n = 1 - \left(x_{n,j} + \frac{1}{2\cdot p^m}\right).$$

For $1 \leq j \leq s$ the j-th components of the points $\boldsymbol{x}_n \in P_{p^m}$ are a 1-dimensional digital net and hence their base p representation has at most m digits unequal zero. Therefore if $x_{n,j} > x_{h,j}$ then we have $x_{n,j} + \delta_n > x_{h,j} + \delta_h$ for arbitrary $\delta_n, \delta_h \in [0, 1/p^m)$. Hence we obtain

$$\begin{aligned} &p^{2m} \int_0^{1/p^m} \int_0^{1/p^m} \min(1-(x_{n,j}+\delta_n), 1-(x_{h,j}+\delta_h)) \mathrm{d}\delta_n \mathrm{d}\delta_h = \\ &\min\left(1 - \left(x_{n,j} + \frac{1}{2\cdot p^m}\right), 1 - \left(x_{h,j} + \frac{1}{2\cdot p^m}\right)\right). \end{aligned}$$

Further we have

$$p^m \int_0^{1/p^m} \frac{1-(x_{n,j}+\delta_n)^2}{2} \mathrm{d}\delta_n = \frac{1}{2}\left(1 - \left(x_{n,j} + \frac{1}{2\cdot p^m}\right)^2\right) - \frac{1}{24\cdot p^{2m}}.$$

Now the result follows from these considerations together with Proposition 1 and the first part of this proof. □

3.2 *An upper bound on the mean square weighted $\mathcal{L}_2$ discrepancy of randomized digital (t,m,s)-nets over $\mathbb{Z}_p$*

In this subsection we derive an upper bound on the formulas shown in Theorem 1. Due to Corollary 1 it is enough to consider in the following only the case that the randomization method is a digital shift of depth m. We have the following theorem.

Theorem 2 *Let P_{p^m} be a digital (t,m,s)-net over $\mathbb{Z}_p$ with $t < m$. Let $\widetilde{P}_{p^m}$ be the point set obtained after applying an i.i.d. random digital shift of depth m independently to each coordinate of each point of P_{p^m}. Then the mean square weighted $\mathcal{L}_2$ discrepancy of $\widetilde{P}_{p^m}$ is bounded by*

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m})] \leq \frac{1}{p^{2m}} \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \left[\frac{1}{6} + p^{2t}\left(\frac{p^2-p+3}{6}\right)^{|\mathfrak{u}|} (m-t)^{|\mathfrak{u}|-1}\right].$$

For $p = 2$ we can recover the result in [4] with the above theorem. Note that using so-called digital sequences (see [12]) it follows that for fixed s and p there always exists a digital (t, m, s)-net over $\mathbb{Z}_p$, where $t \le T(s,p)$ is bounded for some natural number $T(s,p)$ independent of m, and m can be chosen arbitrarily large. Hence the above theorem shows that we can obtain a convergence rate of the root mean square $\mathcal{L}_2$ discrepancy of $O((\log p^m)^{(s-1)/2} p^{-m})$.

Further the upper bound is better for smaller p, hence it is best for $p = 2$. This supports the belief that nets in base 2 yield the best distribution properties.

We need two lemmas for the proof of the above theorem.

Lemma 6 *For any real number $b > 1$ and any integers $k, t_0 > 0$, we have*

$$\sum_{t=t_0}^{\infty} \binom{t+k-1}{k-1} b^{-t} \le b^{-t_0} \binom{t_0+k-1}{k-1} \left(1 - \frac{1}{b}\right)^{-k}.$$

Proof. See [4] or [10]. □

Lemma 7 *Let $C_1, \ldots, C_s$ be the generating matrices of a digital (t, m, s)-net over $\mathbb{Z}_p$. Further define $\mathcal{B}$ as in Theorem 1. Then for any $\mathfrak{v} \subseteq D$ we have*

$$\mathcal{B}(\mathfrak{v}) \le \frac{p^{2t}}{p^{2m}} \left(\frac{p^3}{3(p+1)}\right)^{|\mathfrak{v}|} \left(m - t + \frac{1}{p^3}\right)^{|\mathfrak{v}|-1}.$$

Proof. To simplify the notation we show the result only for $\mathfrak{v} = \{1, \ldots, s\}$. The other cases follow by the same arguments. We have, for $k_j = k_{j,0} + k_{j,1}p + \cdots + k_{j,r_j}p^{r_j}$ and $k_{j,r_j} \neq 0$, $j = 1, 2, \ldots, s$,

$$\begin{aligned}
&\mathcal{B}(\{1, \ldots, s\}) \\
&= \underbrace{\sum_{k_1=1}^{p^m-1} \cdots \sum_{k_s=1}^{p^m-1}}_{C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s = \vec{0}} \prod_{j=1}^{s} \frac{1}{p^{2(r_j+1)}} \left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)} - \frac{1}{3}\right) \\
&= \frac{1}{p^{2s}} \sum_{r_1,\ldots,r_s=0}^{m-1} \frac{1}{p^{2(r_1+\cdots+r_s)}} \underbrace{\sum_{k_1=p^{r_1}}^{p^{r_1+1}-1} \cdots \sum_{k_s=p^{r_s}}^{p^{r_s+1}-1}}_{C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s = \vec{0}} \prod_{j=1}^{s} \left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)} - \frac{1}{3}\right). \qquad (5)
\end{aligned}$$

For $1 \le j \le s$ and $1 \le i \le m$ let $\vec{c}_{j,i}^{\,\top}$ denote the i-th row vector of the matrix C_j. Hence the condition in our sum (5) can be written as

$$\begin{aligned}
&\vec{c}_{1,1}k_{1,0}+\cdots+\vec{c}_{1,r_1}k_{1,r_1-1}+\vec{c}_{1,r_1+1}k_{1,r_1}+\\
&\vec{c}_{2,1}k_{2,0}+\cdots+\vec{c}_{2,r_2}k_{2,r_2-1}+\vec{c}_{2,r_2+1}k_{2,r_2}+\\
&\qquad\qquad\qquad\qquad\qquad\qquad\vdots\\
&\vec{c}_{s,1}k_{s,0}+\cdots+\vec{c}_{s,r_s}k_{s,r_s-1}+\vec{c}_{s,r_s+1}k_{s,r_s}\quad=\vec{0}.
\end{aligned}\tag{6}$$

Since by the digital (t,m,s)-net property (see Definition 1) the vectors

$$\vec{c}_{1,1},\ldots,\vec{c}_{1,r_1+1},\ldots,\vec{c}_{s,1},\ldots,\vec{c}_{s,r_s+1}$$

are linearly independent as long as $(r_1+1)+\cdots+(r_s+1)\le m-t$, we must have

$$r_1+\cdots+r_s\ge m-t-s+1. \tag{7}$$

Let now A denote the $m\times(r_1+\cdots+r_s)$ matrix with the column vectors given by $\vec{c}_{1,1},\ldots,\vec{c}_{1,r_1},\ldots,\vec{c}_{s,1},\ldots,\vec{c}_{s,r_s}$, i.e.,

$$A:=(\vec{c}_{1,1},\ldots,\vec{c}_{1,r_1},\ldots,\vec{c}_{s,1},\ldots,\vec{c}_{s,r_s}).$$

Further let

$$\vec{f}_{k_{1,r_1},\ldots,k_{s,r_s}}:=-(\vec{c}_{1,r_1+1}k_{1,r_1}+\ldots+\vec{c}_{s,r_s+1}k_{s,r_s})\in\mathbb{Z}_p^m$$

and

$$\vec{k}:=(k_{1,0},\ldots,k_{1,r_1-1},\ldots,k_{s,0},\ldots,k_{s,r_s-1})^\top\in\mathbb{Z}_p^{r_1+\cdots+r_s}.$$

Then the linear equation system (6) can be written as

$$A\vec{k}=\vec{f}_{k_{1,r_1},\ldots,k_{s,r_s}} \tag{8}$$

and hence

$$\begin{aligned}
&\underbrace{\sum_{k_1=p^{r_1}}^{p^{r_1+1}-1}\cdots\sum_{k_s=p^{r_s}}^{p^{r_s+1}-1}}_{C_1^\top\vec{k}_1+\cdots+C_s^\top\vec{k}_s=\vec{0}}\prod_{j=1}^{s}\left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)}-\frac{1}{3}\right)\\
&=\sum_{k_{1,r_1},\ldots,k_{s,r_s}=1}^{p-1}\prod_{j=1}^{s}\left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)}-\frac{1}{3}\right)\sum_{\substack{\vec{k}\in\mathbb{Z}_p^{r_1+\cdots+r_s}\\ A\vec{k}=\vec{f}_{k_{1,r_1},\ldots,k_{s,r_s}}}}1\\
&=\sum_{k_{1,r_1},\ldots,k_{s,r_s}=1}^{p-1}\prod_{j=1}^{s}\left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)}-\frac{1}{3}\right)\#\{\vec{k}\in\mathbb{Z}_p^{r_1+\cdots+r_s}:A\vec{k}=\vec{f}_{k_{1,r_1},\ldots,k_{s,r_s}}\}.
\end{aligned}$$

By the definition of the matrix A and since $C_1,\ldots,C_s$ are the generating matrices of a digital (t,m,s)-net over $\mathbb{Z}_p$ we have

$$\operatorname{rank}(A)=\begin{cases}r_1+\cdots+r_s & \text{if } r_1+\cdots+r_s\le m-t,\\ \ge m-t & \text{else.}\end{cases}$$

Let L denote the linear space of solutions of the homogeneous system $A\vec{k}=\vec{0}$ and let $\dim(L)$ denote the dimension of L. Then it follows that

$$\dim(L) = \begin{cases} 0 & \text{if } r_1+\cdots+r_s \leq m-t, \\ \leq r_1+\cdots+r_s-m+t & \text{else.} \end{cases}$$

Hence if $r_1+\cdots+r_s \leq m-t$ we find that the system (8) has at most 1 solution and if $r_1+\cdots+r_s > m-t$ the system (8) has at most $p^{r_1+\cdots+r_s-m+t}$ solutions, i.e.,

$$\begin{aligned}
&\underbrace{\sum_{k_1=p^{r_1}}^{p^{r_1+1}-1} \cdots \sum_{k_s=p^{r_s}}^{p^{r_s+1}-1}}_{C_1^\top \vec{k}_1+\cdots+C_s^\top \vec{k}_s=\vec{0}} \prod_{j=1}^{s} \left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)}-\frac{1}{3}\right) \\
&\leq \sum_{k_{1,r_1},\ldots,k_{s,r_s}=1}^{p-1} \prod_{j=1}^{s} \left(\frac{1}{\sin^2(k_{j,r_j}\pi/p)}-\frac{1}{3}\right) \\
&\qquad\qquad \times \begin{cases} 1 & \text{if } r_1+\cdots+r_s \leq m-t, \\ p^{r_1+\cdots+r_s-m+t} & \text{if } r_1+\cdots+r_s > m-t. \end{cases}
\end{aligned}$$

In [3, Appendix C] it is shown that $\sum_{k=1}^{p-1} \frac{1}{\sin^2(k\pi/p)} = \frac{p^2-1}{3}$. Therefore together with condition (7) we obtain

$$\begin{aligned}
\mathcal{B}(\{1,\ldots,s\}) \leq{}& \frac{1}{p^{2s}}\left(\frac{p^2-p}{3}\right)^s \sum_{\substack{r_1,\ldots,r_s=0 \\ m-t-s+1 \leq r_1+\cdots+r_s \leq m-t}}^{m-1} \frac{1}{p^{2(r_1+\cdots+r_s)}} + \\
&+\frac{1}{p^{2s}}\left(\frac{p^2-p}{3}\right)^s \sum_{\substack{r_1,\ldots,r_s=0 \\ r_1+\cdots+r_s > m-t}}^{m-1} \frac{1}{p^{2(r_1+\cdots+r_s)}} p^{r_1+\cdots+r_s-m+t} \\
&=: \Sigma_1+\Sigma_2. \qquad (9)
\end{aligned}$$

Now we have to estimate the sums Σ_1 and Σ_2. First we have

$$\begin{aligned}
\Sigma_2 &= \left(\frac{p-1}{3p}\right)^s \frac{p^t}{p^m} \sum_{l=m-t+1}^{s(m-1)} \frac{1}{p^l} \sum_{\substack{r_1,\ldots,r_s=0 \\ r_1+\cdots+r_s=l}}^{m-1} 1 \\
&\leq \left(\frac{p-1}{3p}\right)^s \frac{p^t}{p^m} \sum_{l=m-t+1}^{\infty} \binom{l+s-1}{s-1} \frac{1}{p^l},
\end{aligned}$$

where we used the fact that for fixed l the number of non-negative integer solutions of $r_1+\cdots+r_s=l$ is given by $\binom{l+s-1}{s-1}$. Now we apply Lemma 6 and obtain

$$\begin{aligned}\Sigma_2 &\leq \left(\frac{p-1}{3p}\right)^s \frac{p^t}{p^m}\frac{1}{p^{m-t+1}}\binom{m-t+s}{s-1}\left(\frac{p-1}{p}\right)^{-s}\\ &= \frac{1}{3^s}\frac{p^{2t}}{p^{2m}}\frac{1}{p}\binom{m-t+s}{s-1}.\end{aligned}\tag{10}$$

Finally, since

$$\binom{m-t+s}{s-1} = \frac{(m-t+2)(m-t+3)\cdots(m-t+s)}{1\cdot 2\cdots(s-1)} \leq (m-t+2)^{s-1},$$

we obtain

$$\Sigma_2 \leq \frac{1}{3^s}\frac{p^{2t}}{p^{2m}}\frac{1}{p}(m-t+2)^{s-1}.$$

Now we estimate Σ_1. If $m-t \geq s-1$ we proceed similarly to above and obtain

$$\begin{aligned}\Sigma_1 &= \left(\frac{p-1}{3p}\right)^s \sum_{l=m-t-s+1}^{m-t}\binom{l+s-1}{s-1}\frac{1}{p^{2l}}\\ &\leq \left(\frac{p-1}{3p}\right)^s \frac{1}{p^{2(m-t-s+1)}}\binom{m-t}{s-1}\left(1-\frac{1}{p^2}\right)^{-s}\\ &= \frac{1}{3^s}\frac{p^{3s}}{(p+1)^s}\frac{p^{2t}}{p^{2m}}\frac{1}{p^2}\binom{m-t}{s-1}\\ &\leq \frac{1}{3^s}\frac{p^{3s}}{(p+1)^s}\frac{p^{2t}}{p^{2m}}\frac{1}{p^2}\frac{(m-t)^{s-1}}{(s-1)!}.\end{aligned}\tag{11}$$

For this case we obtain

$$\begin{aligned}&\mathcal{B}(\{1,\ldots,s\})\\ &\leq \left(\frac{p^3}{3(p+1)}\right)^s \frac{p^{2t}}{p^{2m}}\left(\frac{1}{p^2}\frac{(m-t)^{s-1}}{(s-1)!} + \frac{1}{p}\frac{(p+1)^s}{p^{3s}}(m-t+2)^{s-1}\right)\\ &= \frac{p^{3s}}{3^s(p+1)^s}\frac{p^{2t}}{p^{2m}}\left(\frac{1}{p^2}\frac{(m-t)^{s-1}}{(s-1)!} + \frac{p+1}{p^4}\left(\frac{p+1}{p^3}(m-t)+\frac{2(p+1)}{p^3}\right)^{s-1}\right).\end{aligned}$$

As $\frac{p+1}{p^3}(m-t)+\frac{2(p+1)}{p^3} \leq m-t+\frac{1}{p^3}$ provided that $m-t>0$ we have

$$\mathcal{B}(\{1,\ldots,s\}) \leq \frac{p^{2t}}{p^{2m}}\cdot\frac{p^{3s}}{3^s\,(p+1)^s}\left(m-t+\frac{1}{p^3}\right)^{s-1}$$

which is the desired bound.

Now we consider the case where $m-t<s-1$. We have

$$\begin{aligned}\Sigma_1 &= \left(\frac{p-1}{3p}\right)^s \sum_{l=0}^{m-t} \binom{l+s-1}{s-1} \frac{1}{p^{2l}} \\ &\le \left(\frac{p-1}{3p}\right)^s \sum_{l=0}^{\infty} \binom{l+s-1}{s-1} \frac{1}{p^{2l}} \\ &= \frac{1}{3^s}\frac{p^s}{(p+1)^s} \le \frac{1}{p^4}\frac{p^{3s}}{3^s(p+1)^s}\frac{p^{2t}}{p^{2m}}. \end{aligned} \tag{12}$$

Thus we obtain

$$\begin{aligned}&\mathcal{B}(\{1,\ldots,s\}) \\ &\le \frac{1}{p^4}\frac{p^{3s}}{3^s(p+1)^s}\frac{p^{2t}}{p^{2m}} + \frac{1}{3^s}\frac{p^{2t}}{p^{2m}}\frac{1}{p}(m-t+2)^{s-1} \\ &= \frac{p^{3s}}{3^s(p+1)^s}\frac{p^{2t}}{p^{2m}}\left(\frac{1}{p^4} + \frac{p+1}{p^4}\left(\frac{p+1}{p^3}(m-t) + \frac{2(p+1)}{p^3}\right)^{s-1}\right).\end{aligned}$$

The result now follows using the same arguments as above. □

Proof of Theorem 2. We use the formula of Theorem 1 together with Lemma 7 to obtain

$$\begin{aligned}\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m})] \le \sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \Bigg[&\frac{1}{p^m}\cdot\frac{1}{2^{|\mathfrak{u}|}}\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right) \\ &+ \frac{1}{3^{|\mathfrak{u}|}}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\ \mathfrak{v}\neq\emptyset}} \left(\frac{3}{2}\right)^{|\mathfrak{v}|}\frac{p^{2t}}{p^{2m}}\cdot\frac{1}{3^{|\mathfrak{v}|}}\left(\frac{p^3}{p+1}\right)^{|\mathfrak{v}|}\left(m-t+\frac{1}{p^3}\right)^{|\mathfrak{v}|-1}\Bigg].\end{aligned}$$

We have

$$\begin{aligned}&\frac{1}{3^{|\mathfrak{u}|}}\sum_{\substack{\mathfrak{v}\subseteq\mathfrak{u}\\ \mathfrak{v}\neq\emptyset}}\left(\frac{p^3}{2(p+1)}\right)^{|\mathfrak{v}|}\left(m-t+\frac{1}{p^3}\right)^{|\mathfrak{v}|-1} \\ &\le (m-t)^{-1}\left(\frac{1}{3}+\frac{p^3}{6(p+1)}\left(m-t+\frac{1}{p^3}\right)\right)^{|\mathfrak{u}|} \\ &\le \left(\frac{p^2-p+3}{6}\right)^{|\mathfrak{u}|}(m-t)^{|\mathfrak{u}|-1},\end{aligned}$$

provided that $m-t>0$. Since for $x<y$ we have $y^s-x^s = s\zeta^{s-1}(y-x)$ for a $x<\zeta<y$ we have

$$1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|} \le \frac{|\mathfrak{u}|}{3\cdot p^m}.$$

As $\frac{|\mathfrak{u}|}{2^{|\mathfrak{u}|}} \leq \frac{1}{2}$ for $|\mathfrak{u}| \geq 1$ we obtain

$$\begin{aligned} & \frac{1}{p^m \cdot 2^{|\mathfrak{u}|}} \left(1 - \left(1 - \frac{1}{3 \cdot p^m}\right)^{|\mathfrak{u}|}\right) \\ & + \frac{1}{3^{|\mathfrak{u}|}} \frac{p^{2t}}{p^{2m}} \sum_{\substack{\mathfrak{v} \subseteq \mathfrak{u} \\ \mathfrak{v} \neq \emptyset}} \frac{1}{2^{|\mathfrak{v}|}} \left(\frac{p^3}{p+1}\right)^{|\mathfrak{v}|} \left(m - t + \frac{1}{p^3}\right)^{|\mathfrak{v}|-1} \\ & \qquad \leq \frac{1}{p^{2m}} \left[\frac{1}{6} + p^{2t} \left(\frac{p^2 - p + 3}{6}\right)^{|\mathfrak{u}|} (m-t)^{|\mathfrak{u}|-1}\right] \end{aligned} \tag{13}$$

and the result follows. □

In the following corollary we refine the bound in Theorem 2 by including the t-values of the lower dimensional projections. Observe that it follows easily from Definition 1 that any projection of a digital (t, m, s)-net on the coordinates of $\emptyset \neq \mathfrak{u} \subseteq D$ is again a digital $(t_\mathfrak{u}, m, |\mathfrak{u}|)$-net with some $t_\mathfrak{u} \leq t$. In the following we write digital $((t_\mathfrak{u}), m, s)$-net to denote a digital (t, m, s)-net where the projections on $\emptyset \neq \mathfrak{u} \subseteq D$ have quality parameter $t_\mathfrak{u}$. The subsequent corollary can by obtained by using (13).

Corollary 2 *Let P_{p^m} be a digital $((t_\mathfrak{u}), m, s)$-net over $\mathbb{Z}_p$ with $\max_{\emptyset \neq \mathfrak{u} \subseteq D} t_\mathfrak{u} < m$. Let $\widetilde{P}_{p^m}$ be the point set obtained after applying an i.i.d. random digital shift of depth m independently to each coordinate of each point of P_{p^m}. Then the mean square weighted $\mathcal{L}_2$ discrepancy of $\widetilde{P}_{p^m}$ is bounded by*

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m})] \leq \frac{1}{p^{2m}} \sum_{\substack{\mathfrak{u} \subseteq D \\ \mathfrak{u} \neq \emptyset}} \gamma_\mathfrak{u} \left[\frac{1}{6} + p^{2t_\mathfrak{u}} \left(\frac{p^2 - p + 3}{6}\right)^{|\mathfrak{u}|} (m - t_\mathfrak{u})^{|\mathfrak{u}|-1}\right].$$

We close this subsection with a result concerning the proportion of shifts of depth m which yield a digitally shifted net with weighted $\mathcal{L}_2$ discrepancy bounded above by a constant times the bound from Theorem 2. The result follows from Markov's inequality.

Corollary 3 *Let P_{p^m} be a digital (t, m, s)-net over $\mathbb{Z}_p$ with $t < m$. Let $\widetilde{P}_{p^m, \boldsymbol{\sigma}_m}$ be the point set obtained after applying the digital shift $\boldsymbol{\sigma}_m$ of depth m to each point of P_{p^m}. Let*

$$f_{\boldsymbol{\gamma}}(t, m, s, p) := \frac{1}{p^{2m}} \sum_{\substack{\mathfrak{u} \subseteq D \\ \mathfrak{u} \neq \emptyset}} \gamma_\mathfrak{u} \left[\frac{1}{6} + p^{2t} \left(\frac{p^2 - p + 3}{6}\right)^{|\mathfrak{u}|} (m - t)^{|\mathfrak{u}|-1}\right]$$

and let μ be the equiprobable measure on the set of all digital shifts of depth

m. For $c \geq 1$ let $\Lambda_c(P_{p^m}) = \left\{\boldsymbol{\sigma}_m : \mathcal{L}_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m,\boldsymbol{\sigma}_m}) \leq c\sqrt{f_{\boldsymbol{\gamma}}(t,m,s,p)}\right\}$. Then, for any $c \geq 1$ we have

$$\mu\left(\Lambda_c(P_{p^m})\right) > 1 - \frac{1}{c^2}.$$

Proof. The result follows from Theorem 2 together with

$$\begin{aligned}&\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m,\boldsymbol{\sigma}_m})]\\ &> c^2 f_{\boldsymbol{\gamma}}(t,m,s,p)\,\mu\left(\left\{\boldsymbol{\sigma}_m : \mathcal{L}_{2,p^m,\boldsymbol{\gamma}}(\widetilde{P}_{p^m,\boldsymbol{\sigma}_m}) > c\sqrt{f_{\boldsymbol{\gamma}}(t,m,s,p)}\right\}\right).\end{aligned}$$

□

3.3 The Hammersley Net

In this section we compute the mean square weighted $\mathcal{L}_2$ discrepancy of the Hammersley net over $\mathbb{Z}_p$. The Hammersley net over $\mathbb{Z}_p$ is a digital $(0,m,2)$-net over $\mathbb{Z}_p$ generated by the matrices

$$C_1 = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix} \text{ and } C_2 = \begin{pmatrix} 0 & \ldots & 0 & 1 \\ \vdots & \iddots & \iddots & 0 \\ 0 & \iddots & \iddots & \vdots \\ 1 & 0 & \ldots & 0 \end{pmatrix}. \tag{14}$$

The following theorem gives an exact formula for the mean square weighted $\mathcal{L}_2$ discrepancy of the Hammersley net over $\mathbb{Z}_p$.

Theorem 3 *Let H_{p^m} be the Hammersley net over $\mathbb{Z}_p$ with p^m points.*

(1) Let $\widetilde{H}_{p^m}$ be the point set obtained after applying an i.i.d. random digital shift of depth m independently to each coordinate of each point of H_{p^m}. Then the mean square weighted $\mathcal{L}_2$ discrepancy of $\widetilde{H}_{p^m}$ is given by

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{H}_{p^m})] = \gamma_{\{1,2\}}\frac{p^4+5p^2-6}{180p^2}\cdot\frac{m}{p^{2m}} + \frac{1}{p^{2m}}\left(\frac{\gamma_{\{1\}}}{6} + \frac{\gamma_{\{2\}}}{6} + \frac{5\gamma_{\{1,2\}}}{36}\right).$$

(2) Let $\widehat{H}_{p^m}$ be the point set obtained after applying an simplified i.i.d. random digital shift independently to each coordinate of each point of H_{p^m}. Then the mean square weighted $\mathcal{L}_2$ discrepancy of $\widehat{H}_{p^m}$ is given by

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widehat{H}_{p^m})] = \gamma_{\{1,2\}}\frac{p^4+5p^2-6}{180p^2}\cdot\frac{m}{p^{2m}} + \frac{\gamma_{\{1\}}+\gamma_{\{2\}}+\gamma_{\{1,2\}}}{12\cdot p^{2m}} - \frac{\gamma_{\{1,2\}}}{24\cdot p^{4m}}.$$

Remark 1 For $p = 2$ the above formulas are true for all digital $(0, m, 2)$-nets over $\mathbb{Z}_2$ and not only for the Hammersley net over $\mathbb{Z}_2$. This was shown in [4, Theorem 2].

Proof. We only prove the first formula. The second one follows from the first one together with Theorem 1. From Theorem 1 we obtain

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{H}_{p^m})] =$$
$$\sum_{\substack{\mathfrak{u}\subseteq D\\ \mathfrak{u}\neq\emptyset}} \gamma_{\mathfrak{u}} \left[\frac{1}{p^m \cdot 2^{|\mathfrak{u}|}}\left(1-\left(1-\frac{1}{3\cdot p^m}\right)^{|\mathfrak{u}|}\right)+\frac{1}{3^{|\mathfrak{u}|}}\sum_{\substack{\mathfrak{v}\subseteq \mathfrak{u}\\ \mathfrak{v}\neq\emptyset}}\left(\frac{3}{2}\right)^{|\mathfrak{v}|}\mathcal{B}(\mathfrak{v})\right],$$

where for $\mathfrak{v} = \{v_1, \ldots, v_e\}$ we have

$$\mathcal{B}(\mathfrak{v}) = \sum_{\substack{k_1,\ldots,k_e=1\\ C_{v_1}^\top \vec{k}_1+\cdots+C_{v_e}^\top \vec{k}_e=\vec{0}}}^{p^m-1} \prod_{j=1}^{e} \psi(k_j),$$

with

$$\psi(k) = -\frac{1}{p^{2(r+1)}}\left(\frac{1}{3}-\frac{1}{\sin^2(\kappa_r\pi/p)}\right)$$

and $r = r(k)$ is such that $p^{r(k)} \leq k < p^{r(k)+1}$.

Since the matrices C_1 and C_2 are both regular it follows that $\mathcal{B}(\mathfrak{v}) = 0$ if $|\mathfrak{v}| = 1$. Therefore we have

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}}(\widetilde{H}_{p^m})] = \frac{\gamma_{\{1\}}+\gamma_{\{2\}}}{6\cdot p^{2m}}+\frac{\gamma_{\{1,2\}}}{6\cdot p^{2m}}-\frac{\gamma_{\{1,2\}}}{36\cdot p^{3m}}+\frac{\gamma_{\{1,2\}}}{4}\mathcal{B}(\{1,2\}).$$

We consider

$$\mathcal{B}(\{1,2\}) =$$
$$\frac{1}{p^4}\sum_{u,v=0}^{m-1}\frac{1}{p^{2(u+v)}}\underbrace{\sum_{k=p^u}^{p^{u+1}-1}\sum_{l=p^v}^{p^{v+1}-1}}_{C_1^\top\vec{k}+C_2^\top\vec{l}=\vec{0}}\left(\frac{1}{\sin^2(\kappa_u\pi/p)}-\frac{1}{3}\right)\left(\frac{1}{\sin^2(\lambda_v\pi/p)}-\frac{1}{3}\right).$$

Denote by $e_1, \ldots, e_m$ the row vectors of C_1 and by $d_1, \ldots, d_m$ the row vectors of C_2. The condition $C_1^\top\vec{k}+C_2^\top\vec{l} = \vec{0}$ can be rewritten as $e_1\kappa_0+\cdots+e_{u+1}\kappa_u+d_1\lambda_0+\cdots+d_{v+1}\lambda_v = \vec{0}$, where $k = \kappa_0+\kappa_1 p+\cdots+\kappa_u p^u$ and $l = \lambda_0+\lambda_1 p+\cdots+\lambda_v p^v$.

Since $e_1, \ldots, e_{u+1}, d_1, \ldots, d_{v+1}$ are linearly independent as long as $u+1+v+1 \leq m$ we must have $u+v \geq m-1$. Hence

$$\mathcal{B}(\{1,2\}) = \frac{1}{p^4} \sum_{\substack{u,v=0\\u+v\geq m-1}}^{m-1} \frac{1}{p^{2(u+v)}} \underbrace{\sum_{\kappa_u=1}^{p-1} \sum_{\kappa_{u-1},\ldots,\kappa_0=0}^{p-1} \sum_{\lambda_v=1}^{p-1} \sum_{\lambda_{v-1},\ldots,\lambda_0=0}^{p-1}}_{e_1\kappa_0+\cdots+e_{u+1}\kappa_u+d_1\lambda_0+\cdots+d_{v+1}\lambda_v=\vec{0}} \rho(\kappa_u)\rho(\lambda_v),$$

where we write $\rho(\kappa) := \frac{1}{\sin^2(\kappa\pi/p)} - \frac{1}{3}$.

Assume that $u+v=\tau \geq m-1$. Then we have

$$e_1\kappa_0 + \cdots + e_{u+1}\kappa_u + d_1\lambda_0 + \cdots + d_{v+1}\lambda_v = \vec{0}$$

iff

$$\begin{pmatrix} \kappa_0 \\ \vdots \\ \kappa_{m-\tau+u-2} \\ \kappa_{m-\tau+u-1} \\ \vdots \\ \kappa_u \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \lambda_{\tau-u} \\ \vdots \\ \lambda_{m-u-1} \\ \lambda_{m-u-2} \\ \vdots \\ \lambda_0 \end{pmatrix} = \vec{0},$$

i.e., iff

- $\kappa_0 = \cdots = \kappa_{m-\tau+u-2} = 0$ and
- $\lambda_0 = \cdots = \lambda_{m-u-2} = 0$ and
- $\kappa_{m-i-1} = p - \lambda_i$ for $i = m-1-u, \ldots, \tau-u$.

Therefore we have

$$\begin{aligned}\mathcal{B}(\{1,2\}) = {} & \frac{1}{p^4}\frac{1}{p^{2(m-1)}} \sum_{\substack{u,v=0\\u+v=m-1}}^{m-1} \sum_{\kappa_u=1}^{p-1} \rho(\kappa_u)\rho(p-\kappa_u) \\ & + \frac{1}{p^4} \sum_{\tau=m}^{2m-2} \frac{1}{p^{2\tau}} \sum_{\substack{u,v=0\\u+v=\tau}}^{m-1} \sum_{\kappa_u=1}^{p-1} \sum_{\lambda_v=1}^{p-1} \rho(\kappa_u)\rho(\lambda_v) p^{\tau-m}.\end{aligned}$$

For $m-1 \leq \tau \leq 2m-2$ we have

$$\sum_{\substack{u,v=0\\u+v=\tau}}^{m-1} 1 = 2m-\tau-1.$$

Further we have $\rho(p-\kappa_u) = \rho(\kappa_u)$ and hence

$$\mathcal{B}(\{1,2\}) = \frac{m}{p^{2m}} \cdot \frac{1}{p^2} \sum_{k=1}^{p-1} \rho(k)^2 + \frac{1}{p^4 \cdot p^m} \left(\sum_{\tau=m}^{2m-2} \frac{2m-\tau-1}{p^\tau} \right) \left(\sum_{k=1}^{p-1} \rho(k) \right)^2 .$$

From

$$\sum_{\tau=m}^{2m-2} \frac{2m-\tau-1}{p^\tau} = \frac{m}{p^m} \cdot \frac{p}{p-1} + \frac{p^2(1-p^m)}{(p-1)^2 p^{2m}}$$

and

$$\sum_{k=1}^{p-1} \rho(k) = \frac{p^2-p}{3}$$

we obtain

$$\mathcal{B}(\{1,2\}) = \frac{m}{p^{2m}} \cdot \frac{1}{p^2} \sum_{k=1}^{p-1} \rho(k)^2 + \frac{m}{p^{2m}} \cdot \frac{p-1}{9p} + \frac{1-p^m}{9 \cdot p^{3m}}.$$

In [1, Corollary 5.2] it is shown that

$$\sum_{k=1}^{p-1} \frac{1}{\sin^4(k\pi/p)} = \frac{p^4+10p^2-11}{45}.$$

Therefore we have

$$\begin{aligned}
\sum_{k=1}^{p-1} \rho(k)^2 &= \sum_{k=1}^{p-1} \left(\frac{1}{\sin^2(k\pi/p)} - \frac{1}{3} \right)^2 \\
&= \sum_{k=1}^{p-1} \frac{1}{\sin^4(k\pi/p)} - \frac{2}{3} \sum_{k=1}^{p-1} \frac{1}{\sin^2(k\pi/p)} + \frac{p-1}{9} \\
&= \frac{p^4+10p^2-11}{45} - \frac{2p^2-2}{9} + \frac{p-1}{9} = \frac{p^4+5p-6}{45}.
\end{aligned}$$

Hence

$$\begin{aligned}
&\mathcal{B}(\{1,2\}) = \\
&\frac{m}{p^{2m}} \frac{p^4+5p-6}{45p^2} + \frac{m}{p^{2m}} \cdot \frac{p-1}{9p} + \frac{1-p^m}{9 \cdot p^{3m}} = \frac{m}{p^{2m}} \frac{p^4+5p^2-6}{45p^2} + \frac{1-p^m}{9 \cdot p^{3m}}
\end{aligned}$$

and the result follows. □

4 The dependency of the leading constant on the base p

In this section we consider the classical $\mathcal{L}_2$ discrepancy, that is, we choose $\gamma_D = 1$ and $\gamma_{\mathfrak{u}} = 0$ for $\mathfrak{u} \subset D$. We denote this choice of weights by $\boldsymbol{\gamma}_c$. We investigate closer how the leading term as defined in (3) in the bounds for the classical mean square $\mathcal{L}_2$ discrepancy depends on the base p. From the previous section we know that the leading constant for the mean square weighted $\mathcal{L}_2$ discrepancy of 2-dimensional Hammersley nets in base p is given by

$$A(p) = \sqrt{\frac{p^4 + 5p^2 - 6}{180p^2 \log p}}.$$

It can easily be checked that $A(p)$ attains the smallest value by choosing base $p = 2$. This supports the generally believed idea that nets in base 2 yield the smallest discrepancy.

For the general case such a result is difficult to obtain, but the upper bound in the theorem below shows a similar behaviour of the leading constant also in the general case.

In the following we consider the general case, that is, we consider arbitrary digital (t, m, s)-nets over $\mathbb{Z}_p$. For an $s \in \mathbb{N}$ and each $m \in \mathbb{N}$ let $P_{p,t,s,2^m,\boldsymbol{\sigma}_{m,s}}$ be a digital (t, m, s)-net over $\mathbb{Z}_p$ shifted by the digital shift $\boldsymbol{\sigma}_{m,s}$ of depth m. We obtain the following theorem.

Theorem 4 *Let $p \geq 2$, $s > 3$, $0 \leq t < m$ and $m - t \geq s$ be such that a digital (t, m, s)-net over $\mathbb{Z}_p$ exists. Then there exists a digital shift $\boldsymbol{\sigma}_{m,s}$ of depth m such that for the shifted net $P_{p,t,s,p^m,\boldsymbol{\sigma}_{m,s}}$ we have*

$$\mathcal{L}_{2,p^m,\boldsymbol{\gamma}_c}(P_{p,t,s,p^m,\boldsymbol{\sigma}_{m,s}}) \leq \frac{p^t}{p^m}\sqrt{\binom{m-t+s}{s-1}} \left(\frac{p^3}{6(p+1)}\right)^{s/2} \frac{\sqrt{2}}{p} + O\left(\frac{m^{(s-2)/2}}{2^m}\right).$$

Proof. We obtain from Theorem 1

$$\mathbb{E}[\mathcal{L}^2_{2,p^m,\boldsymbol{\gamma}_c}(\widetilde{P}_{p^m})] = \frac{1}{p^m 2^s}\left(1 - \left(1 - \frac{1}{3p^m}\right)^s\right) + \frac{1}{3^s}\sum_{\substack{\mathfrak{v} \subseteq D \\ \mathfrak{v} \neq \emptyset}} \left(\frac{3}{2}\right)^{|\mathfrak{v}|} \mathcal{B}(\mathfrak{v}). \qquad (15)$$

Lemma 7 shows that, in order to find the constant of the leading term, we only need to consider $\mathcal{B}(\{1, \ldots, s\})$. From (9), (10) and (11) we obtain

$$\mathcal{B}(\{1, \ldots, s\}) \leq \frac{p^{2t}}{p^{2m}} \frac{1}{3^s p}\left(\binom{m-t+s}{s-1} + \frac{p^{3s}}{p(p+1)^s}\binom{m-t}{s-1}\right).$$

As the bound in Theorem 1 was obtained by averaging over all shifts it follows that there exists a shift which yields an $\mathcal{L}_2$ discrepancy smaller than or equal to this bound. The result follows. □

Since $\binom{m-t+s}{s-1} = O(m^{s-1})$ it follows that the constant in the upper bound (i.e., the upper bound on $A(p)$) increases at least with $p^s(\log p)^{-s/2}$. It might be possible to improve this bound for special choices of nets, as shown for the case of Hammersley nets above, but in general we expect the constant to grow with the base p. Hence the best bound can be obtained for $p = 2$. This special case, i.e., $p = 2$, was analyzed in detail in [4].

References

[1] Berndt, B.C., and Yeap, B.P., Explicit evaluations and reciprocity theorems for finite trigonometric sums. Adv. in Appl. Math., **29**: 358–385, 2002.

[2] Chrestenson, H.E., A class of generalized Walsh functions. Pacific J. Math., **5**: 17–31, 1955.

[3] Dick, J., and Pillichshammer, F., Multivariate integration in weighted Hilbert spaces based on Walsh functions and weighted Sobolev spaces. J. Complexity, **21**: 149–195, 2005.

[4] Dick, J., and Pillichshammer, F., On the mean square weighted $\mathcal{L}_2$ discrepancy of randomized digital (t, m, s)-nets over $\mathbb{Z}_2$. Acta Arith., **117**: 371–403, 2005.

[5] Drmota, M., and Tichy, R.F., *Sequences, discrepancies and applications.* Lecture Notes in Mathematics 1651, Springer Verlag, Berlin, 1997.

[6] Kuipers, L., and Niederreiter, H., *Uniform Distribution of Sequences.* John Wiley, New York, 1974.

[7] Larcher, G., Digital point sets: analysis and application. In: *Random and Quasi-Random Point Sets*, Hellekalek, P., and Larcher, G., editors. Springer Lecture Notes in Statistics 138, 167–222, 1998.

[8] Larcher, G., Niederreiter, H., and Schmid, W.Ch., Digital nets and sequences constructed over finite rings and their application to quasi-Monte Carlo integration. Monatsh. Math., **121**: 231–253, 1996.

[9] Leobacher, G., and Pillichshammer, F., Bounds for the weighted L^p discrepancy and tractability of integration. J. Complexity, **19**: 529–547, 2003.

[10] Matoušek, J., *Geometric Discrepancy.* Algorithms and Combinatorics 18, Springer Verlag, Berlin, 1999.

[11] Niederreiter, H., Point sets and sequences with small discrepancy. Monatsh. Math., **104**: 273–337, 1987.

[12] Niederreiter, H., *Random Number Generation and Quasi-Monte Carlo Methods.* No. 63 in CBMS-NSF Series in Applied Mathematics, SIAM, Philadelphia, 1992.

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

[14] Owen, A.B., Randomly permuted (t, m, s)-nets and (t, s)-sequences. Monte Carlo and quasi-Monte Carlo methods in scientific computing (Las Vegas, NV, 1994), Lecture Notes in Statist. 106, 299–317, Springer, New York, 1995.

[15] Pirsic, G., Schnell konvergierende Walshreihen über Gruppen. Master's Thesis, University of Salzburg, 1995. (Available at http://www.ricam.oeaw.ac.at/people/page/pirsic/)

[16] Rivlin, T.J., and Saff, E.B., *Joseph L. Walsh Selected Papers.* Springer Verlag, New York, 2000.

[17] Roth, K.F., On irregularities of distribution. Mathematika, **1**: 73–79, 1954.

[18] Sloan, I.H., and Woźniakowski, H., When are quasi-Monte Carlo algorithms efficient for high dimensional integrals? J. Complexity, **14**: 1–33, 1998.

[19] Walsh, J.L., A closed set of normal orthogonal functions. Amer. J. Math., **55**: 5–24, 1923.

[20] Warnock, T.T., Computational investigations of low discrepancy point sets. In: Zaremba S.K. (Ed.), *Applications of Number Theory to Numerical Analysis*, Academic Press, New York, 319–343, 1972.

[21] Yue, R.X., and Hickernell, F.J., The discrepancy and gain coefficients of scrambled digital nets. J. Complexity, **18**: 135–151, 2002.