ACTA ARITHMETICA
162.1 (2014)

Optimal $\mathcal{L}_2$ discrepancy bounds for higher order digital sequences over the finite field $\mathbb{F}_2$

by

Josef Dick (Sydney) and Friedrich Pillichshammer (Linz)

1. Introduction and statement of the main results. We study equidistribution properties of point sets in the s-dimensional unit-cube $[0,1)^s$ measured by their $\mathcal{L}_2$ discrepancy (see [2, 15, 18, 26, 31]). For a finite set $\mathcal{P}_{N,s} = \{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{N-1}\}$ of points in the s-dimensional unit-cube $[0,1)^s$ the *local discrepancy function* is defined as

$$\Delta(t_1, \dots, t_s) = \frac{A_N([\mathbf{0}, \boldsymbol{t}), \mathcal{P}_{N,s})}{N} - t_1 \cdots t_s,$$

where $\boldsymbol{t} = (t_1, \dots, t_s) \in [0,1]^s$ and $A_N([\mathbf{0}, \boldsymbol{t}), \mathcal{P}_{N,s})$ denotes the number of indices n with $\boldsymbol{x}_n \in [0, t_1) \times \cdots \times [0, t_s) =: [\mathbf{0}, \boldsymbol{t})$. The discrepancy function measures the difference of the portion of points in an axis parallel box containing the origin and the volume of this box. Hence it is a measure of the irregularity of distribution of a point set in $[0,1)^s$.

The $\mathcal{L}_2$ *discrepancy* of $\mathcal{P}_{N,s}$ is defined as

$$\mathcal{L}_{2,N}(P_{N,s}) = \Big(\int_{[0,1]^s} |\Delta(\boldsymbol{t})|^2 \, d\boldsymbol{t} \Big)^{1/2}. \tag{1}$$

For an infinite sequence $\mathcal{S}_s = (\boldsymbol{x}_0, \boldsymbol{x}_1, \dots)$ in $[0,1)^s$ the $\mathcal{L}_2$ discrepancy $\mathcal{L}_{2,N}(\mathcal{S}_s)$ is the $\mathcal{L}_2$ discrepancy of the first N elements of $\mathcal{S}_s$.

It is well known that a sequence is uniformly distributed modulo one if and only if its $\mathcal{L}_2$ discrepancy tends to zero for growing N. Furthermore, the $\mathcal{L}_2$ discrepancy can also be linked to the integration error of a quasi-Monte Carlo rule; see e.g. [15, 32, 46] for the error in the worst case setting and [52] for the average case setting.

A lower bound on the $\mathcal{L}_2$ discrepancy of *finite* point sets has been shown by Roth [39]: for any $s \in \mathbb{N}$ (the set of positive integers) there exists a

2010 *Mathematics Subject Classification*: Primary 11K38; Secondary 11K06, 11K45, 65C05.

Key words and phrases: $\mathcal{L}_2$ discrepancy, explicit constructions, digital sequence, higher order sequence, digital higher order sequence, higher order net, higher order digital net.

DOI: 10.4064/aa162-1-4

number $c_s > 0$, depending only on s, such that for every point set $\mathcal{P}_{N,s}$ in $[0,1)^s$ consisting of $N \geq 2$ points we have

$$\mathcal{L}_{2,N}(\mathcal{P}_{N,s}) \geq c_s \frac{(\log N)^{(s-1)/2}}{N}. \tag{2}$$

This lower bound is best possible in the order of magnitude in N, as shown first by Davenport [10] for $s = 2$ and then by Roth [40, 41] for arbitrary dimensions $s \in \mathbb{N}$. Other constructions of point sets with optimal $\mathcal{L}_2$ discrepancy were found by Chen [4, 5], Dobrovol'skiĭ [17], Frolov [23] and Skriganov [42, 43]. Davenport used point sets consisting of the $2N$ elements $(\{\pm n\alpha\}, n/N)$ for $1 \leq n \leq N$, where $N \in \mathbb{N}$ and α has a continued fraction expansion with bounded partial quotients. Further examples of two-dimensional point sets with best possible order of $\mathcal{L}_2$ discrepancy can be found in [19, 20, 21, 25, 27, 37]. On the other hand, Roth's [41] proof for dimensions $s \geq 2$ is a pure existence result obtained by averaging arguments as are the constructions in [4, 5, 17, 23, 42, 43]. Explicit constructions of point sets achieving the best possible order of convergence have been a longstanding open problem. Finally, a solution was given by Chen and Skriganov [7] who, for every integer $N \geq 2$ and every dimension $s \in \mathbb{N}$, gave for the first time explicit constructions of finite point sets consisting of N points in $[0,1)^s$ whose $\mathcal{L}_2$ discrepancy achieves an order of convergence of $(\log N)^{(s-1)/2}/N$. Their construction uses a finite field $\mathbb{F}_p$ of order p with $p \geq 2s^2$. We also refer to [8] where the arguments from [7] are considerably simplified, and to the overview in [15, Chapter 16]. The result in [7] was extended to the $\mathcal{L}_p$ discrepancy for $1 \leq p < \infty$ by Skriganov [44]. See also [45] where a construction over $\mathbb{F}_2$ was studied.

On the other hand, it was shown by Proinov [36] that for an infinite sequence $\mathcal{S}_s$ of points in $[0,1)^s$ there is a constant $c'_s > 0$ such that

$$\mathcal{L}_{2,N}(\mathcal{S}_s) \geq c'_s \frac{(\log N)^{s/2}}{N}$$

for infinitely many values of N. This lower bound is known to be best possible in dimension $s = 1$. One-dimensional infinite sequences whose $\mathcal{L}_2$ discrepancy satisfies a bound of order $\sqrt{\log N}/N$ for every $N \geq 2$ were given in, e.g., [3, 24, 27, 36, 38]. These constructions are mainly based on the symmetrization of sequences (also called reflection principle). On the other hand, although it was widely believed that Proinov's lower bound is also best possible for arbitrary dimensions s, so far there was no proof for this assertion.

1.1. The main results. In this paper we prove two main results: We provide for the first time explicit constructions of *infinite* sequences in $[0,1)^s$ for which the first $N \geq 2$ points achieve an $\mathcal{L}_2$ discrepancy of order

$(\log N)^{s/2}/N$ for arbitrary $s \in \mathbb{N}$. This result is best possible by the lower bound of Proinov [36].

Furthermore, for any integer $N \geq 2$ and any dimension $s \in \mathbb{N}$, we give an explicit construction of a finite point set of N elements in the s-dimensional unit cube with the optimal rate of convergence for the $\mathcal{L}_2$ discrepancy in the sense of the lower bound of Roth. Our construction is different from that of Chen and Skriganov [7]. In contrast to [7] where the construction uses a finite field $\mathbb{F}_p$ with $p \geq 2s^2$, our method is, independently of the dimension s, based on the finite field $\mathbb{F}_2$ of order two. Furthermore, our result does not use the Davenport reflection principle [10] and also does not use the 'self-averaging' property from [7]. Instead it is based on higher order digital nets and sequences from [11, 12].

In our proofs we do not keep track of constants which depend only on the dimension s since they are significantly larger than the constants obtained in [14]. Therefore, in the following, we write $A(N,s) \ll_s B(N,s)$ if there is a constant $c_s > 0$ which depends only on s (and not on N or m through $N = 2^m$) such that $A(N,s) \leq c_s B(N,s)$.

THEOREM 1.1. *For any $s \in \mathbb{N}$ one can explicitly construct an infinite sequence $\mathcal{S}_s$ of points in $[0,1)^s$ such that for all $N \geq 2$ we have*

$$\mathcal{L}_{2,N}(\mathcal{S}_s) \ll_s \frac{(\log N)^{(s-1)/2}}{N} \sqrt{S(N)} \ll_s \frac{(\log N)^{s/2}}{N},$$

where $S(N)$ is the sum-of-digits function of N in base 2 representation, i.e., if $N = 2^{m_1} + \cdots + 2^{m_r}$ with $m_1 > \cdots > m_r \geq 0$, then $S(N) = r$. Obviously, we have $S(N) \leq 1 + (\log N)/(\log 2)$ for all $N \in \mathbb{N}$.

REMARK 1.2. It follows from [28, Corollary 3] that for any $\varepsilon > 0$ we have

$$\lim_{M \to \infty} \frac{1}{M} \left| \left\{ 0 \leq N < M : (1-\varepsilon)\frac{\log M}{2 \log 2} < S(N) < (1+\varepsilon)\frac{\log M}{2 \log 2} \right\} \right| = 1.$$

Hence the density of $N \in \mathbb{N}$ for which $S(N)$ is at least of order $\log N$ is equal to one. More precise results on the distribution of the sum-of-digits function can be obtained, e.g., from [1, 30].

The above construction can also be used to obtain the following result for finite point sets, which was first shown in [7] by a different construction.

COROLLARY 1.3. *For any $s \in \mathbb{N}$ and any integer $N \geq 2$ one can explicitly construct a point set $\mathcal{P}_{N,s}$ consisting of N elements in $[0,1)^s$ such that*

$$\mathcal{L}_{2,N}(\mathcal{P}_{N,s}) \ll_s \frac{(\log N)^{(s-1)/2}}{N}.$$

A comparison of the approach in this paper with the method used in [7] can be found in [16].

1.2. Explicit constructions of sequences and point sets. We now present explicit constructions of sequences and point sets satisfying Theorem 1.1 and Corollary 1.3. For $p \in \mathbb{N}$ let $\mathbb{Q}(2^p) := \{0, \frac{1}{2^p}, \frac{2}{2^p}, \ldots, \frac{2^p-1}{2^p}\}$.

The construction of sequences $\mathcal{S}_s = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots)$ in $[0,1)^s$ satisfying Theorem 1.1 was introduced in [11, 12] and is based on linear algebra over the finite field $\mathbb{F}_2$ of order 2 (we identify $\mathbb{F}_2$ with the set $\{0,1\}$ equipped with the arithmetic operations modulo 2).

First we need to recall the definition of digital nets according to Niederreiter [33, 34]: For $m, p \in \mathbb{N}$ with $p \geq m$ let $C_1, \ldots, C_s \in \mathbb{F}_2^{p \times m}$ be $p \times m$ matrices over $\mathbb{F}_2$. For $n \in \{0, \ldots, 2^m - 1\}$ with binary expansion $n = n_0 + n_1 2 + \cdots + n_{m-1} 2^{m-1}$ we define the binary digit vector $\vec{n}$ as $\vec{n} = (n_0, n_1, \ldots, n_{m-1})^\top \in \mathbb{F}_2^m$ (the symbol $\top$ means the transpose of a vector or a matrix). Then compute

$$C_j \vec{n} =: (x_{j,n,1}, x_{j,n,2}, \ldots, x_{j,n,p})^\top \quad \text{for } j = 1, \ldots, s,$$

where the matrix vector product is evaluated over $\mathbb{F}_2$, and put

$$x_{j,n} = x_{j,n,1} 2^{-1} + x_{j,n,2} 2^{-2} + \cdots + x_{j,n,p} 2^{-p} \in \mathbb{Q}(2^p).$$

The nth point $\boldsymbol{x}_n$ of the net $\mathcal{P}_{2^m,s}$ is given by $\boldsymbol{x}_n = (x_{1,n}, \ldots, x_{s,n})$. A net $\mathcal{P}_{2^m,s}$ constructed this way is called a *digital net* (*over* $\mathbb{F}_2$) *with generating matrices* $C_1, \ldots, C_s$. Note that a digital net consists of 2^m elements in $\mathbb{Q}(2^p)^s$.

We also recall the definition of digital sequences according to Niederreiter [33, 34], which are infinite versions of digital nets. Let $C_1, \ldots, C_s \in \mathbb{F}_2^{\mathbb{N} \times \mathbb{N}}$ be $\mathbb{N} \times \mathbb{N}$ matrices over $\mathbb{F}_2$. For $C_j = (c_{j,k,\ell})_{k,\ell \in \mathbb{N}}$ we assume that for each $\ell \in \mathbb{N}$ there exists a $K(\ell) \in \mathbb{N}$ such that $c_{j,k,\ell} = 0$ for all $k > K(\ell)$. For $n \in \mathbb{N}_0$, where $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, with binary expansion $n = n_0 + n_1 2 + \cdots + n_{m-1} 2^{m-1} \in \mathbb{N}_0$, we define the infinite dyadic digit vector of n by $\vec{n} = (n_0, n_1, \ldots, n_{m-1}, 0, 0, \ldots)^\top \in \mathbb{F}_2^{\mathbb{N}}$. Then compute

$$C_j \vec{n} =: (x_{j,n,1}, x_{j,n,2}, \ldots)^\top \quad \text{for } j = 1, \ldots, s,$$

where the matrix vector product is evaluated over $\mathbb{F}_2$, and put

$$x_{j,n} = x_{j,n,1} 2^{-1} + x_{j,n,2} 2^{-2} + \cdots \in [0,1).$$

The nth point $\boldsymbol{x}_n$ of the sequence $\mathcal{S}_s$ is given by $\boldsymbol{x}_n = (x_{1,n}, \ldots, x_{s,n})$. A sequence $\mathcal{S}_s$ constructed this way is called a *digital sequence* (*over* $\mathbb{F}_2$) *with generating matrices* $C_1, \ldots, C_s$. Note that since $c_{j,k,\ell} = 0$ for all k large enough, the numbers $x_{j,n}$ are always dyadic rationals. (We call $x \in [0,1)$ a *dyadic rational* if it can be written as a finite base 2 expansion.)

Explicit constructions of suitable generating matrices $C_1, \ldots, C_s$ over $\mathbb{F}_2$ were obtained by Sobol' [47], Niederreiter [33, 34], Niederreiter–Xing [35]

and others (see [15, Chapter 8] for an overview). For completeness, we briefly describe a special case of Tezuka's construction [49], which is a generalization of Sobol's construction [47] and Niederreiter's construction [33] of the generating matrices.

We explain how to construct the entries $c_{j,k,\ell} \in \mathbb{F}_2$ of the generator matrices $C_j = (c_{j,k,\ell})_{k,\ell \geq 1}$ for $j = 1, \ldots, s$. To this end choose the polynomials $p_1 = x$ and $p_j \in \mathbb{F}_2[x]$ for $j = 2, \ldots, s$ to be the $(j-1)$th primitive polynomial in a list of primitive polynomials over $\mathbb{F}_2$ that is sorted in increasing order according to their degree $e_j = \deg(p_j)$, that is, $e_2 \leq e_3 \leq \cdots \leq e_s$ (the ordering of polynomials with the same degree is irrelevant). We also put $e_1 = \deg(x) = 1$. (We point out that Niederreiter [33] uses irreducible polynomials instead of primitive polynomials.)

Let $j \in \{1, \ldots, s\}$ and $k \in \mathbb{N}$. Take $i-1$ and z to be respectively the main term and remainder when we divide $k-1$ by e_j, so that $k-1 = (i-1)e_j + z$, with $0 \leq z < e_j$. Now consider the Laurent series expansion

$$\frac{x^{e_j - z - 1}}{p_j(x)^i} = \sum_{\ell=1}^{\infty} a_\ell(i,j,z) x^{-\ell} \in \mathbb{F}_2((x^{-1})).$$

For $\ell \in \mathbb{N}$ we set

$$c_{j,k,\ell} = a_\ell(i,j,z). \tag{3}$$

Every digital sequence with generating matrices $C_j = (c_{j,k,\ell})_{k,\ell \geq 1}$ for $j = 1, \ldots, s$ found in this way is a special instance of a Sobol' sequence, which, in turn, is a special instance of so-called generalized Niederreiter sequences (see [49, eq. (3)]). Note that in the construction above we always have $c_{j,k,\ell} = 0$ for all $k > \ell$.

Observe that *generalized Niederreiter sequences* (as are Sobol's and Niederreiter's sequences) are digital (t,s)-sequences with

$$t = \sum_{j=1}^{s} (e_j - 1). \tag{4}$$

See [49, Lemma 4] for details.

To obtain a sequence which satisfies Theorem 1.1 we need the following definition.

Definition 1.4. For $\alpha \in \mathbb{N}$ the *digit interlacing composition* (with interlacing factor α) is defined by

$$\mathscr{D}_\alpha : [0,1)^\alpha \to [0,1), \qquad (x_1, \ldots, x_\alpha) \mapsto \sum_{a=1}^{\infty} \sum_{r=1}^{\alpha} \xi_{r,a} 2^{-r-(a-1)\alpha},$$

where $x_r \in [0,1)$ has dyadic expansion of the form $x_r = \xi_{r,1} 2^{-1} + \xi_{r,2} 2^{-2} + \cdots$ for $1 \leq r \leq \alpha$. We also define this function for vectors by setting

$$\mathscr{D}_\alpha^s : [0,1)^{\alpha s} \to [0,1)^s,$$
$$(x_1,\ldots,x_{\alpha s}) \mapsto (\mathscr{D}_\alpha(x_1,\ldots,x_\alpha),\ldots,\mathscr{D}_\alpha(x_{(s-1)\alpha+1},\ldots,x_{\alpha s})),$$

for point sets $\mathcal{P}_{N,\alpha s} = \{\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{N-1}\} \subseteq [0,1)^{\alpha s}$ by setting

$$\mathscr{D}_\alpha^s(\mathcal{P}_{N,\alpha s}) = \{\mathscr{D}_\alpha^s(\boldsymbol{x}_0),\mathscr{D}_\alpha^s(\boldsymbol{x}_1),\ldots,\mathscr{D}_\alpha^s(\boldsymbol{x}_{N-1})\} \subseteq [0,1)^s$$

and for sequences $\mathcal{S}_{\alpha s} = (\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots)$ with $\boldsymbol{x}_n \in [0,1)^{\alpha s}$ by setting

$$\mathscr{D}_\alpha^s(\mathcal{S}_{\alpha s}) = (\mathscr{D}_\alpha^s(\boldsymbol{x}_0),\mathscr{D}_\alpha^s(\boldsymbol{x}_1),\ldots).$$

We comment here that the interlacing can also be applied to the generating matrices $C_1,\ldots,C_{\alpha s}$ directly as described in [12, Section 4.4]: Let $C_1,\ldots,C_{\alpha s}$ be generating matrices of a digital net or sequence and let $\vec{c}_{j,k}$ denote the kth row of C_j. We define matrices $E_1,\ldots,E_s$, where the kth row of E_j is given by $\vec{e}_{j,k}$, in the following way. For all $1 \le j \le s$, $u \ge 0$ and $1 \le v \le \alpha$ let

$$\vec{e}_{j,u\alpha+v} = \vec{c}_{(j-1)\alpha+v,u+1}.$$

If $C_1,\ldots,C_{\alpha s}$ are the generating matrices of a digital net $\mathcal{P}_{N,\alpha s}$ or digital sequence $\mathcal{S}_{\alpha s}$ respectively, then the matrices $E_1,\ldots,E_s$ defined above are the generating matrices of $\mathscr{D}_\alpha^s(\mathcal{P}_{N,\alpha s})$ or $\mathscr{D}_\alpha^s(\mathcal{S}_{\alpha s})$ respectively. Thus one can also obtain generating matrices $E_1,\ldots,E_s \in \mathbb{F}_2^{\mathbb{N}\times\mathbb{N}}$ which generate a digital sequence satisfying Theorem 1.1.

Above we assumed that $c_{j,k,\ell} = 0$ for all $k > K(\ell)$. Let $E_j = (e_{j,k,\ell})_{k,\ell\in\mathbb{N}}$. Then the interlacing construction yields $e_{j,k,\ell} = 0$ for all $k > \alpha K(\ell)$, where α is the interlacing factor.

We shall show that the sequence $\mathscr{D}_5^s(\mathcal{S}_{5s})$, where $\mathcal{S}_{5s}$ is a digital sequence in dimension $5s$ constructed for example according to Sobol' as presented above, satisfies the bounds in Theorem 1.1.

To construct finite point sets for any integer $N \ge 2$ we proceed in the following way. Let $m \in \mathbb{N}$ be such that $2^{m-1} < N \le 2^m$ and let $\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{2^m-1} \in [0,1]^{3s-1}$ be the first 2^m points from the sequence in dimension $3s-1$ as introduced above with $p_1 = x$ and $p_2 = 1+x$. Let $\boldsymbol{x}_n = (x_{1,n},\ldots,x_{3s-1,n})$ and define the point $\boldsymbol{y}_n = (n2^{-m},x_{1,n},\ldots,x_{3s-1,n}) \in [0,1)^{3s}$. Let now

$$\mathcal{P}_{2^m,s} = \{\mathscr{D}_3(\boldsymbol{y}_0),\mathscr{D}_3(\boldsymbol{y}_1),\ldots,\mathscr{D}_3(\boldsymbol{y}_{2^m})\}.$$

To obtain a point set consisting of N points we use a propagation rule introduced in [7] (see also [15, p. 512]): The subset

$$\widetilde{\mathcal{P}}_{N,s} := \mathcal{P}_{2^m,s} \cap \left(\left[0,\frac{N}{2^m}\right) \times [0,1)^{s-1}\right)$$

contains exactly N points. Then we define the point set

$$\mathcal{P}_{N,s} := \left\{ \left(\frac{2^m}{N} x_1, x_2, \dots, x_s \right) : (x_1, x_2, \dots, x_s) \in \widetilde{\mathcal{P}}_{N,s} \right\}. \tag{5}$$

We will show that $\mathcal{P}_{N,s}$ satisfies the bound in Corollary 1.3. We remark that Chen and Skriganov [7] applied the same propagation rule but to a different point set.

1.3. The general construction principle. Our approach is based on higher order digital nets and sequences constructed explicitly in [11, 12]. We state here simplified versions of their definitions that are sufficient for our purpose.

The distribution quality of digital nets and sequences depends on the choice of the respective generating matrices. In the following definitions we put some restrictions on $C_1, \dots, C_s$ with the aim to quantify the quality of equidistribution of the digital net or sequence.

DEFINITION 1.5. Let $m, p, \alpha \in \mathbb{N}$ with $p \geq \alpha m$ and let t be an integer such that $0 \leq t \leq \alpha m$. Let $C_1, \dots, C_s \in \mathbb{F}_2^{p \times m}$ with $C_j = (\vec{c}_{j,1}, \dots, \vec{c}_{j,p})^\top$, i.e., $\vec{c}_{j,i} \in \mathbb{F}_2^m$ is the ith row vector of the matrix C_j. If for all $1 \leq i_{j,\nu_j} < \cdots < i_{j,1} \leq p$ with

$$\sum_{j=1}^{s} \sum_{l=1}^{\min(\nu_j, \alpha)} i_{j,l} \leq \alpha m - t$$

the vectors

$$\vec{c}_{1,i_{1,\nu_1}}, \dots, \vec{c}_{1,i_{1,1}}, \dots, \vec{c}_{s,i_{s,\nu_s}}, \dots, \vec{c}_{s,i_{s,1}}$$

are linearly independent over $\mathbb{F}_2$, then the digital net with generating matrices $C_1, \dots, C_s$ is called an *order α digital (t, m, s)-net over $\mathbb{F}_2$*.

Next we consider digital sequences for which the initial segments are order α digital (t, m, s)-nets over $\mathbb{F}_2$:

DEFINITION 1.6. Let $\alpha \in \mathbb{N}$ and let $t \geq 0$ be an integer. Let $C_1, \dots, C_s \in \mathbb{F}_2^{\mathbb{N} \times \mathbb{N}}$ and let $C_{j,\alpha m \times m}$ denote the left upper $\alpha m \times m$ submatrix of C_j. If for all $m > t/\alpha$ the matrices $C_{1,\alpha m \times m}, \dots, C_{s,\alpha m \times m}$ generate an order α digital (t, m, s)-net over $\mathbb{F}_2$, then the digital sequence with generating matrices $C_1, \dots, C_s$ is called an *order α digital (t, s)-sequence over $\mathbb{F}_2$*.

From Definition 1.5 it is clear that if $\mathcal{P}_{2^m,s}$ is an order α digital (t, m, s)-net, then for any $t \leq t' \leq \alpha m$, $\mathcal{P}_{2^m,s}$ is also an order α digital (t', m, s)-net. An analogous result also applies to higher order digital sequences.

From [11, Theorems 4.11 and 4.12] (where we set $\alpha = d$) we obtain the following result:

PROPOSITION 1.7. *If $\mathcal{S}_{\alpha s}$ is an order 1 digital $(t', \alpha s)$-sequence over $\mathbb{F}_2$, then $\mathscr{D}^s_\alpha(\mathcal{S}_{\alpha s})$ is an order α digital (t, s)-sequence over $\mathbb{F}_2$ with*

$$t = \alpha t' + s\binom{\alpha}{2}.$$

For the construction based on Sobol's and Niederreiter's sequence introduced above we have (4) and therefore we obtain explicit constructions of order α digital (t, s)-sequences with

$$t = \alpha \sum_{j=1}^{s} (e_j - 1) + s\binom{\alpha}{2}.$$

Note that in the construction introduced above we have $c_{j,k,\ell} = 0$ for all $k > \ell$. Using the interlacing construction we obtain generating matrices $E_1, \dots, E_s$ with $E_j = (e_{j,k,\ell})_{k,\ell \in \mathbb{N}}$ and $e_{j,k,\ell} = 0$ for all $k > \alpha\ell$. Let $E_{j,\mathbb{N}\times m}$ denote the first m columns of E_j. Then we see that the kth row of $E_{j,\mathbb{N}\times m}$ is the zero-vector for all $k > \alpha m$. This implies that the first 2^m points of the digital sequence with generating matrices $E_1, \dots, E_s$ are the same as the points of the digital net with generating matrices $E_{1,\alpha m\times m}, \dots, E_{s,\alpha m\times m}$. In particular this implies that all coordinates of all points are dyadic rationals. (For more general constructions of digital (t, s)-sequences a similar result holds, however we do not use this fact here.)

Note that a digital net can be an order α digital (t, m, s)-net over $\mathbb{F}_2$ and at the same time an order α' digital (t', m, s)-net over $\mathbb{F}_2$ for $\alpha' \neq \alpha$. This means that the quality parameter t may depend on α. If necessary we write $t(\alpha)$ instead of t for the quality parameter of an order α digital $(t(\alpha), m, s)$-net. The same holds for digital sequences. In particular, [12, Theorem 4.10] implies that an order α digital (t, m, s)-net is an order α' digital (t', m, s)-net for all $1 \le \alpha' \le \alpha$ with

$$t' = \lceil t\alpha'/\alpha \rceil \le t. \tag{6}$$

The same result applies to order α digital (t, s)-sequences which are also order $1 \le \alpha' \le \alpha$ digital (t', s)-sequences with t' as above. In other words, $t(\alpha') = \lceil t(\alpha)\alpha'/\alpha \rceil$ for all $1 \le \alpha' \le \alpha$. More information can be found in [15, Chapter 15].

We will show that every order α digital (t, s)-sequence over $\mathbb{F}_2$ with $\alpha \ge 5$ satisfies the requirements of Theorem 1.1.

1.4. Geometric properties of (higher order) digital nets. We give a geometric interpretation of the digital nets introduced above. For $\alpha = 1$ they go back to Niederreiter [33, 34]. The condition in Definition 1.5 says

that so-called dyadic elementary boxes of the form

$$\prod_{j=1}^{s}\left[\frac{a_j}{2^{d_j}},\frac{a_j+1}{2^{d_j}}\right),$$

with integers $d_j \geq 0$, $d_1+\cdots+d_s = m-t$, and integers $0 \leq a_j < 2^{d_j}$, contain b^t points of the net, which is the fair portion of points of the net with respect to the volume of the box. Thus smaller values of the so-called quality parameter t imply stronger equidistribution properties of a net. For more information see [34, Theorem 4.28] or [15, Theorem 4.52].

The more general definition for $\alpha > 1$ goes back to Dick [11, 12]. Rather than considering boxes containing the right portion of points as for the case $\alpha = 1$, here one considers unions of such boxes. To give geometric interpretation, we define for $\nu \in \mathbb{N}_0$, $a_1 > \cdots > a_\nu \geq -\nu+1$ and $\kappa_1,\ldots,\kappa_\nu \in \{0,1\}$ the union of intervals

$$J_\alpha(a_1,\ldots,a_\nu,\kappa_1,\ldots,\kappa_\nu) = \left\{x \in [0,1) : x = \sum_{d=1}^{\infty}\xi_d 2^{-d} \text{ with } \xi_{a_i} = \kappa_i \text{ for } i = 1,\ldots,\nu\right\},$$

where we set $J = [0,1)$ for $\nu = 0$, where $a_i \in \{-\nu+1, -\nu+2,\ldots,0\}$ does not yield any restriction and where we always use the finite expansion of x for dyadic rationals. For instance we have $J_2(0,-1,0,0) = [0,1)$, $J_2(1,0,0,0) = [0,1/2)$ and $J_2(3,1,1,1) = [5/8,6/8)\cup[7/8,1)$. Let $1_J(x)$ denote the indicator function of a set J (that is, 1 for $x \in J$ and 0 otherwise). Then an order α digital (t,m,s)-net satisfies

$$\sum_{n=0}^{2^m-1} 1_J(\boldsymbol{x}_n) = \text{Volume}(J)$$

for all J of the form

$$\prod_{j=1}^{s} J_\alpha(a_{1,j},\ldots,a_{\nu_j,j},\kappa_{1,j},\ldots,\kappa_{\nu_j,j})$$

for all $\kappa_{r,j} \in \{0,1\}$, all $1 \leq r \leq \nu_j$ and $1 \leq j \leq s$, and all $a_{j,1} > a_{j,2} > \cdots > a_{j,\nu_j} > -\nu_j+1$ with

$$\sum_{j=1}^{s}\sum_{r=1}^{\min\{\nu_j,\alpha\}} \max\{a_{j,r},0\} \leq \alpha m - t.$$

Thus higher order digital nets contain the correct proportion of points not only for elementary dyadic intervals, but also for certain unions of disjoint dyadic intervals. Thus higher order digital nets have an additional structure which classical digital nets do not necessarily have.

2. Walsh series representation of the squared $\mathcal{L}_2$ discrepancy. As an important tool in our analysis we use a Walsh series representation of the $\mathcal{L}_2$ discrepancy. This representation will be deduced within this chapter.

2.1. Walsh functions. We introduce Walsh functions in base 2 (see [9, 22, 50]), which will be the main tool in our analysis of the $\mathcal{L}_2$ discrepancy. We recall that $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

For $k \in \mathbb{N}_0$ the *kth Walsh function* $\mathrm{wal}_k : [0,1) \to \{-1,1\}$ is defined in the following way: let k have base 2 representation

$$k = \kappa_{a-1} 2^{a-1} + \cdots + \kappa_1 2 + \kappa_0,$$

with $\kappa_i \in \{0,1\}$, and let $x \in [0,1)$ have base 2 representation

$$x = \frac{\xi_1}{2} + \frac{\xi_2}{2^2} + \cdots$$

with $\xi_i \in \{0,1\}$ (unique in the sense that infinitely many of the ξ_i must be zero); then

$$\mathrm{wal}_k(x) := (-1)^{\xi_1 \kappa_0 + \cdots + \xi_a \kappa_{a-1}}.$$

For dimension $s \geq 2$, 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

$$\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}) := \prod_{j=1}^{s} \mathrm{wal}_{k_j}(x_j).$$

A summary of properties of Walsh functions can be found in [15, Appendix A]. See also [6] for Walsh functions in the context of discrepancy theory, [29] for Walsh functions in the related context of numerical integration in [29], or [48] in the related context of pseudo random number generation.

We report on a relation between Walsh functions and digital nets over $\mathbb{F}_2$ which will be useful for our analysis. Before we do so we need to introduce some further notation. By $\oplus$ we denote the digit-wise addition modulo 2, i.e., for real numbers $x, y \geq 0$ with dyadic expansion $x = \sum_{i=w}^{\infty} \xi_i / 2^i$ and $y = \sum_{i=w}^{\infty} \eta_i / 2^i$ with $w \in \mathbb{Z}$ and $\xi_i \neq 1$ for infinitely many i and $\eta_j \neq 1$ for infinitely many j, we put

$$x \oplus y := \sum_{i=w}^{\infty} \frac{\zeta_i}{2^i}, \quad \text{where } \zeta_i := \xi_i + \eta_i \,(\mathrm{mod}\ 2).$$

For vectors $\boldsymbol{x}, \boldsymbol{y} \in [0,1)^s$ we set $\boldsymbol{x} \oplus \boldsymbol{y} = (x_1 \oplus y_1, \ldots, x_s \oplus y_s)$. Note that e.g. for $x = 2^{-1} + 2^{-3} + 2^{-5} + \cdots$ and $y = 2^{-2} + 2^{-4} + 2^{-6} + \cdots$ we have $x \oplus y = 2^{-1} + 2^{-2} + 2^{-3} + \cdots = 1$ (see [22, Section 2]). Thus $x \oplus y$ is a dyadic rational which is not defined via its finite expansion. However, in this paper, we only use $\oplus$ in conjunction with dyadic rationals x and y for which we assume that x and y are given by their finite expansion. Therefore,

in this paper, $x \oplus y$ will always be a dyadic rational defined via its finite expansion.

It can be shown (see [15, Lemma 4.72]) that any digital net $\mathcal{P}_{2^m,s}$ is a subgroup of $([0,1)^s, \oplus)$. Since for any $\boldsymbol{x}_h, \boldsymbol{x}_j \in \mathcal{P}_{2^m,s}$ and any $\boldsymbol{k} \in \mathbb{N}_0^s$ we have

$$\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_h \oplus \boldsymbol{x}_j) = \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_h)\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_j)$$

it follows that $\mathrm{wal}_{\boldsymbol{k}}$ is a character of the group $(\mathcal{P}_{2^m,s}, \oplus)$. Hence, for any digital net $\mathcal{P}_{2^m,s}$ with generating matrices $C_1, \ldots, C_s \in \mathbb{F}_2^{p\times m}$ and any $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathbb{N}_0^s$ it follows that

$$\sum_{h=0}^{2^m-1} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_h) = \begin{cases} 2^m & \text{if } C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s = \vec{0}, \\ 0 & \text{otherwise,} \end{cases} \tag{7}$$

where for $k_j \in \mathbb{N}_0$ with dyadic expansion $k_j = \kappa_{j,0} + \kappa_{j,1}2 + \cdots + \kappa_{j,a-1}2^{a-1}$ we set $\vec{k}_j = (\kappa_{j,0}, \kappa_{j,1}, \ldots, \kappa_{j,p-1})^\top$ with $\kappa_{j,a} = \kappa_{j,a+1} = \cdots = \kappa_{j,p-1} = 0$ for $a < p$. For a proof of this fact we refer to [13, Lemma 4.75] (there only $p = m$ was considered, but only minor modifications are required to obtain a proof of (7)). We will call this relation the *character property* of digital nets.

2.2. The Walsh series expansion of the $\mathcal{L}_2$ discrepancy. The squared $\mathcal{L}_2$ discrepancy of a point set $\mathcal{P}_{N,s} = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ can be viewed as a function of $\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$, i.e. a function of Ns variables:

$$\mathcal{L}_{2,N}^2(\mathcal{P}_{N,s}) = \mathcal{L}_{2,N}^2(\{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}).$$

To obtain its Walsh series expansion, we use the following well known formula of Warnock [51] (see also [15, Proposition 2.15]).

PROPOSITION 2.1. *Let $\mathcal{P}_{N,s} = \{\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{N-1}\}$ be a point set in $[0,1)^s$. Then*

$$\mathcal{L}_{2,N}^2(\mathcal{P}_{N,s}) = \frac{1}{3^s} - \frac{2}{N}\sum_{n=0}^{N-1}\prod_{j=1}^{s}\frac{1-x_{n,j}^2}{2} + \int_{[0,1]^s}\left(\frac{A_N([\boldsymbol{0},\boldsymbol{t}),\mathcal{P}_{N,s})}{N}\right)^2 d\boldsymbol{t},$$

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

We need the Walsh series expansion of the indicator function $1_{[0,t)}(x)$, first given by Fine [22] and nowadays well known. To state this expansion we need a weight function μ defined for non-negative integers. Put $\mu(0) = 0$ and for $k \in \mathbb{N}$ with base 2 representation $k = \kappa_0 + \kappa_1 2 + \cdots + \kappa_{a-2}2^{a-2} + 2^{a-1}$ with $\kappa_i \in \{0,1\}$ put $\mu(k) := a$.

Then for $x \in [0,1]$ the Walsh series expansion of $1_{[0,t)}(x)$ is given as

$$1_{[0,t)}(x) \simeq 1 - x + \sum_{k=1}^{\infty} \frac{1}{2^{\mu(k)+1}} \left(\sum_{r=1}^{\infty} \frac{1}{2^r} \operatorname{wal}_{k \oplus 2^{r+\mu(k)-1}}(x) - \operatorname{wal}_{k \oplus 2^{\mu(k)-1}}(x) \right) \operatorname{wal}_k(t).$$

Using Parseval's identity we therefore obtain

$$\begin{aligned} &\int_0^1 1_{[0,t)}(x) 1_{[0,t)}(y)\, dt \\ &= (1-x)(1-y) + \sum_{k=1}^{\infty} \frac{1}{2^{2\mu(k)+2}} \left(\operatorname{wal}_{k \oplus 2^{\mu(k)-1}}(x) - \sum_{r=1}^{\infty} \frac{1}{2^r} \operatorname{wal}_{k \oplus 2^{r+\mu(k)-1}}(x) \right) \\ &\qquad \times \left(\operatorname{wal}_{k \oplus 2^{\mu(k)-1}}(y) - \sum_{r=1}^{\infty} \frac{1}{2^r} \operatorname{wal}_{k \oplus 2^{r+\mu(k)-1}}(y) \right). \end{aligned}$$

Using the fact that $A_N([\mathbf{0}, \boldsymbol{t}), \mathcal{P}_{N,s}) = \sum_{n=0}^{N-1} \prod_{j=1}^{s} 1_{[0,t_j)}(x_{n,j})$ we find that

$$\int_{[0,1]^s} \left(\frac{A_N([\mathbf{0}, \boldsymbol{t}), \mathcal{P}_{N,s})}{N} \right)^2 d\boldsymbol{t} = \frac{1}{N^2} \sum_{n,m=0}^{N-1} \prod_{j=1}^{s} \int_0^1 1_{[0,t_j)}(x_{n,j}) 1_{[0,t_j)}(x_{m,j})\, dt_j.$$

Combining the last two equations we obtain

$$\begin{aligned} &\int_{[0,1]^s} \left(\frac{A_N([\mathbf{0}, \boldsymbol{t}), \mathcal{P}_{N,s})}{N} \right)^2 d\boldsymbol{t} \\ &= \frac{1}{N^2} \sum_{n,m=0}^{N-1} \prod_{j=1}^{s} \Bigg[(1 - x_{n,j})(1 - x_{m,j}) \\ &\quad + \sum_{k=1}^{\infty} \frac{1}{2^{2\mu(k)+2}} \left(\operatorname{wal}_{k \oplus 2^{\mu(k)-1}}(x_{n,j}) - \sum_{r=1}^{\infty} \frac{1}{2^r} \operatorname{wal}_{k \oplus 2^{r+\mu(k)-1}}(x_{n,j}) \right) \\ &\quad \times \left(\operatorname{wal}_{k \oplus 2^{\mu(k)-1}}(x_{m,j}) - \sum_{r=1}^{\infty} \frac{1}{2^r} \operatorname{wal}_{k \oplus 2^{r+\mu(k)-1}}(x_{m,j}) \right) \Bigg]. \end{aligned} \tag{8}$$

The Walsh series representation of $(1 - x_{n,j})(1 - x_{m,j})$ can easily be found. For example it was shown in [15, Lemma A.22] that

$$x - \frac{1}{2} = -\sum_{a=1}^{\infty} \frac{1}{2^{a+1}} \operatorname{wal}_{2^{a-1}}(x). \tag{9}$$

Using (8) together with the last equality we obtain the Walsh series representation of $\int_{[0,1]^s} (A_N([\mathbf{0}, \boldsymbol{t}), \mathcal{P}_{N,s})/N)^2\, d\boldsymbol{t}$.

Using (9) again and Proposition 2.1 we can now obtain the Walsh series expansion of the squared $\mathcal{L}_2$ discrepancy:

$$
\begin{aligned}
(10)\qquad \mathcal{L}_{2,N}^2(\mathcal{P}_{N,s}) = \frac{1}{3^s} - \frac{2}{N}\sum_{n=0}^{N-1}\prod_{j=1}^{s}\Bigg(\frac{1}{3} + \sum_{a=1}^{\infty}\frac{1}{2^{a+2}}\operatorname{wal}_{2^{a-1}}(x_{n,j}) \\
- \sum_{1\le a<a'}\frac{1}{2^{a+a'+2}}\operatorname{wal}_{2^{a-1}\oplus 2^{a'-1}}(x_{n,j})\Bigg) \\
+ \frac{1}{N^2}\sum_{n,m=0}^{N-1}\prod_{j=1}^{s}\Bigg[\Bigg(\frac{1}{2} + \sum_{a=1}^{\infty}\frac{1}{2^{a+1}}\operatorname{wal}_{2^{a-1}}(x_{n,j})\Bigg) \\
\times \Bigg(\frac{1}{2} + \sum_{a=1}^{\infty}\frac{1}{2^{a+1}}\operatorname{wal}_{2^{a-1}}(x_{m,j})\Bigg) \\
+ \sum_{k=1}^{\infty}\frac{1}{2^{2\mu(k)+2}}\Bigg(\operatorname{wal}_{k\oplus 2^{\mu(k)-1}}(x_{n,j}) - \sum_{r=1}^{\infty}\frac{1}{2^r}\operatorname{wal}_{k\oplus 2^{r+\mu(k)-1}}(x_{n,j})\Bigg) \\
\times \Bigg(\operatorname{wal}_{k\oplus 2^{\mu(k)-1}}(x_{m,j}) - \sum_{r=1}^{\infty}\frac{1}{2^r}\operatorname{wal}_{k\oplus 2^{r+\mu(k)-1}}(x_{m,j})\Bigg)\Bigg].
\end{aligned}
$$

The following lemma can now be obtained upon comparing coefficients.

LEMMA 2.2. *For any $\mathcal{P}_{N,s} = \{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{N-1}\}$ in $[0,1)^s$ we obtain*

$$
\begin{aligned}
\mathcal{L}_{2,N}^2(\mathcal{P}_{N,s}) = \frac{1}{3^s} - \frac{2}{N}\sum_{n=0}^{N-1}\sum_{\boldsymbol{k}\in\mathbb{N}_0^s} r(\boldsymbol{k},\boldsymbol{0})\operatorname{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) \\
+ \frac{1}{N^2}\sum_{n,m=0}^{N-1}\sum_{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s} r(\boldsymbol{k},\boldsymbol{l})\operatorname{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\operatorname{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m),
\end{aligned}
$$

where $\boldsymbol{k} = (k_1, \dots, k_s)$, $\boldsymbol{l} = (l_1, \dots, l_s)$, $r(\boldsymbol{k},\boldsymbol{l}) = \prod_{j=1}^{s} r(k_j, l_j)$. Furthermore, $r(k,l) = r(l,k)$ and for non-negative integers $0 \le l \le k$ with $k = 2^{a_1-1} + \cdots + 2^{a_v-1}$ with $a_1 > \cdots > a_v > 0$ and $l = 2^{b_1-1} + \cdots + 2^{b_w-1}$ with $b_1 > \cdots > b_v > 0$ we have

$$
r(k,l) = \begin{cases}
1/3 & \text{if } k = l = 0, \\
1/2^{a_1+2} & \text{if } v = 1 \text{ and } l = 0, \\
-1/2^{a_1+a_2+2} & \text{if } v = 2 \text{ and } l = 0, \\
-1/2^{a_1+a_2+2} & \text{if } v = w+2 > 2 \text{ and } a_3 = b_1, \dots, a_v = b_{v-2}, \\
1/(3\cdot 4^{a_1}) & \text{if } k = l > 0, \\
1/2^{a_1+b_1+2} & \text{if } v = w,\ a_1 \ne b_1 \text{ and } a_2 = b_2, \dots, a_v = b_v, \\
0 & \text{otherwise.}
\end{cases}
$$

Proof. As already mentioned, the result follows from (10) upon comparing coefficients. For instance we have

$$\frac{1}{3}+\sum_{a=1}^{\infty}\frac{1}{2^{a+2}}\operatorname{wal}_{2^{a-1}}(x_{n,j})-\sum_{1\le a<a'}\frac{1}{2^{a+a'+2}}\operatorname{wal}_{2^{a-1}\oplus 2^{a'-1}}(x_{n,j})=\sum_{k=0}^{\infty}r(k,0)\operatorname{wal}_k(x_{n,j})$$

with

$$r(k,0)=\begin{cases}1/3 & \text{if } k=0,\\ 1/2^{a+2} & \text{if } k=2^{a-1},\\ -1/2^{a+a'+2} & \text{if } k=2^{a-1}\oplus 2^{a'-1},\\ 0 & \text{in all other cases.}\end{cases}$$

Now it suffices to check all cases. ∎

We can simplify the above formula further. But first we recall what we mean by a digitally shifted digital net:

Definition 2.3. Let $\mathcal{P}_{2^m,s}=\{\boldsymbol{x}_0,\dots,\boldsymbol{x}_{2^m-1}\}$ be a digital net over $\mathbb{F}_2$ and let $\boldsymbol{\sigma}\in[0,1)^s$. Then we call the point set $\mathcal{P}_{2^m,s}(\boldsymbol{\sigma})=\{\boldsymbol{x}_0\oplus\boldsymbol{\sigma},\dots,\boldsymbol{x}_{2^m-1}\oplus\boldsymbol{\sigma}\}$ a *digitally shifted digital net over* $\mathbb{F}_2$.

In this paper we will only consider digital shifts which are dyadic rationals. Since the points of a digital net are also dyadic rationals, the operation $\oplus$ is well defined.

Lemma 2.4.

- *The squared $\mathcal{L}_2$ discrepancy of a point set $\mathcal{P}_{N,s}=\{\boldsymbol{x}_0,\dots,\boldsymbol{x}_{N-1}\}$ in $[0,1)^s$ can be written as*

$$\mathcal{L}_{2,N}^2(\mathcal{P}_{N,s})=\sum_{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s\setminus\{\boldsymbol{0}\}}r(\boldsymbol{k},\boldsymbol{l})\frac{1}{N}\sum_{n=0}^{N-1}\operatorname{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\frac{1}{N}\sum_{m=0}^{N-1}\operatorname{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m),$$

  where the coefficients $r(\boldsymbol{k},\boldsymbol{l})$ are given as in Lemma 2.2.
- *If $\mathcal{P}_{2^m,s}$ is a digital net over $\mathbb{F}_2$ with generating matrices $C_1,\dots,C_s\in\mathbb{F}_2^{p\times m}$ then*

$$\mathcal{L}_{2,2^m}^2(\mathcal{P}_{2^m,s})=\sum_{\boldsymbol{k},\boldsymbol{l}\in\mathcal{D}^*}r(\boldsymbol{k},\boldsymbol{l}),$$

  where $\mathcal{D}^*=\mathcal{D}\setminus\{\boldsymbol{0}\}$ and $\mathcal{D}$ is the so-called dual net given by

$$\mathcal{D}=\{(k_1,\dots,k_s)\in\mathbb{N}_0^s:C_1^\top\vec{k}_1+\cdots+C_s^\top\vec{k}_s=\vec{0}\},$$

  where for $k\in\mathbb{N}_0^s$ with base 2 expansion $k=\kappa_0+\kappa_1 2+\kappa_2 2^2+\cdots$ we put $\vec{k}=(\kappa_0,\dots,\kappa_{p-1})^\top$.

- *If $\mathcal{P}_{2^m,s}(\boldsymbol{\sigma})$ is a digital net over $\mathbb{F}_2$ digitally shifted by the digital shift $\boldsymbol{\sigma}$ then*

$$\mathcal{L}^2_{2,2^m}(\mathcal{P}_{2^m,s}(\boldsymbol{\sigma})) = \sum_{\boldsymbol{k},\boldsymbol{l}\in\mathcal{D}^*} r(\boldsymbol{k},\boldsymbol{l})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{\sigma})\,\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{\sigma}),$$

where $\mathcal{D}^*$ denotes the dual net excluding $\mathbf{0}$.

Proof. From $r(\mathbf{0},\mathbf{0}) = 3^{-s}$ and from the symmetry relation $r(\boldsymbol{k},\boldsymbol{l}) = r(\boldsymbol{l},\boldsymbol{k})$ we obtain

$$\begin{aligned}
\mathcal{L}^2_{2,N}(\mathcal{P}_{N,s}) &= \frac{1}{3^s} - \frac{2}{N}\sum_{n=0}^{N-1}\sum_{\boldsymbol{k}\in\mathbb{N}_0^s} r(\boldsymbol{k},\mathbf{0})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\\
&\quad + \frac{1}{N^2}\sum_{n,m=0}^{N-1}\sum_{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s} r(\boldsymbol{k},\boldsymbol{l})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\,\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m)\\
&= r(\mathbf{0},\mathbf{0}) - 2r(\mathbf{0},\mathbf{0}) + r(\mathbf{0},\mathbf{0}) - \frac{1}{N^2}\sum_{n,m=0}^{N-1}\sum_{\boldsymbol{k}\in\mathbb{N}^s} r(\boldsymbol{k},\mathbf{0})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\\
&\quad - \frac{1}{N^2}\sum_{n,m=0}^{N-1}\sum_{\boldsymbol{l}\in\mathbb{N}^s} r(\mathbf{0},\boldsymbol{l})\,\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m)\\
&\quad + \frac{1}{N^2}\sum_{n,m=0}^{N-1}\sum_{\substack{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s\\(\boldsymbol{k},\boldsymbol{l})\neq(\mathbf{0},\mathbf{0})}} r(\boldsymbol{k},\boldsymbol{l})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\,\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m)\\
&= \frac{1}{N^2}\sum_{n,m=0}^{N-1}\sum_{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s\setminus\{\mathbf{0}\}} r(\boldsymbol{k},\boldsymbol{l})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\,\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m)\\
&= \sum_{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s\setminus\{\mathbf{0}\}} r(\boldsymbol{k},\boldsymbol{l})\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n)\frac{1}{N}\sum_{m=0}^{N-1}\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m),
\end{aligned}$$

which proves the first part. The second part follows immediately from the first part and the character property (7) of digital nets. The third part follows in the same manner as the second part using the additional equality $\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}\oplus\boldsymbol{\sigma}) = \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{\sigma})$. ∎

3. The proof of Theorem 1.1. We give the proof of our main result. Throughout this proof we assume that $\alpha \geq 3$ unless stated otherwise. We consider the construction of digital sequences $\mathcal{S}_{\alpha s}$ based on (3) in dimension αs and apply the digit interlacing function $\mathscr{D}^s_\alpha(\mathcal{S}_{\alpha s})$ of order α. The sequence $\mathcal{S}_s := \mathscr{D}^s_\alpha(\mathcal{S}_{\alpha s}) := (\boldsymbol{x}_0,\boldsymbol{x}_1,\ldots)$ in $[0,1)^s$ is an order α digital (t,s)-sequence with $t = \alpha\sum_{j=1}^s (e_j-1) + s\binom{\alpha}{2}$. Using (6), $\mathscr{D}^s_\alpha(\mathcal{S}_{\alpha s})$ is also an order α' digital

(t', s)-sequence with $t' = \lceil t\alpha'/\alpha \rceil \le t$ for all $1 \le \alpha' \le \alpha$. Thus it is also an order α' digital (t, s)-sequence for all $1 \le \alpha' \le \alpha$; see Subsection 1.3 for more details. Note that we have $t \ge s\binom{\alpha}{2} \ge \binom{3}{2} = 3$.

Let $C_1, \ldots, C_s$ denote the generating matrices of the digital sequence $\mathcal{S}_s$. Let $C_{j,\mathbb{N}\times m}$ denote the first m columns of C_j. As explained in Subsection 1.3, only the first αm rows of $C_{j,\mathbb{N}\times m}$ can be non-zero and hence C_j is of the form

$$C_j = \left(\begin{array}{c|c} C_{j,\alpha m\times m} & D_{j,\alpha m\times \mathbb{N}} \\ \hline 0_{\mathbb{N}\times m} & F_{j,\mathbb{N}\times\mathbb{N}} \end{array}\right) \in \mathbb{F}_2^{\mathbb{N}\times\mathbb{N}},$$

where $0_{\mathbb{N}\times m}$ denotes the $\mathbb{N} \times m$ zero matrix. Note that the entries of each column of the matrix $F_{j,\mathbb{N}\times\mathbb{N}}$ become eventually zero.

We use the first part of Lemma 2.4 to obtain

$$\mathcal{L}^2_{2,N}(\mathcal{S}_s) = \sum_{\boldsymbol{k},\boldsymbol{l}\in\mathbb{N}_0^s\setminus\{\boldsymbol{0}\}} r(\boldsymbol{k},\boldsymbol{l}) \frac{1}{N}\sum_{n=0}^{N-1} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) \frac{1}{N}\sum_{m=0}^{N-1} \mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{x}_m). \tag{11}$$

Let $N = 2^{m_1} + \cdots + 2^{m_r}$ with $m_1 > \cdots > m_r \ge 0$ (hence $r = S(N)$). We consider the point sets

$$\mathcal{P}_i := \{\boldsymbol{x}_{2^{m_1}+\cdots+2^{m_i}-1}, \ldots, \boldsymbol{x}_{-1+2^{m_1}+\cdots+2^{m_i}}\},$$

for $i = 1, \ldots, r$, where for $i = 1$ we define $2^{m_1} + \cdots + 2^{m_{i-1}} = 0$. Any $n \in \{2^{m_1} + \cdots + 2^{m_{i-1}}, \ldots, -1 + 2^{m_1} + \cdots + 2^{m_i}\}$ can be written in the form

$$n = 2^{m_1} + \cdots + 2^{m_{i-1}} + a = 2^{m_{i-1}}\ell + a$$

with $a \in \{0, 1, \ldots, 2^{m_i} - 1\}$ and $\ell = 1 + 2^{m_i - m_{i-1}} + \cdots + 2^{m_1 - m_{i-1}}$ if $i > 1$ and $\ell = 0$ for $i = 1$. Hence the dyadic digit vector of n is given by

$$\vec{n} = (a_0, a_1, \ldots, a_{m_i-1}, l_0, l_1, l_2, \ldots)^\top =: \begin{pmatrix} \vec{a} \\ \vec{\ell} \end{pmatrix},$$

where $a_0, \ldots, a_{m_i-1}$ are the dyadic digits of a and $l_0, l_1, l_2, \ldots$ are the dyadic digits of ℓ. With this notation we have

$$C_j\vec{n} = \begin{pmatrix} C_{j,\alpha m_i\times m_i}\vec{a} \\ 0 \\ 0 \\ \vdots \end{pmatrix} + \begin{pmatrix} D_{j,\alpha m\times\mathbb{N}} \\ \hline F_{j,\mathbb{N}\times\mathbb{N}} \end{pmatrix} \vec{\ell}.$$

For the point set $\mathcal{P}_i$ under consideration, the vector

$$\vec{\sigma}_{i,j} := \begin{pmatrix} D_{j,\alpha m\times\mathbb{N}} \\ \hline F_{j,\mathbb{N}\times\mathbb{N}} \end{pmatrix} \vec{\ell} \tag{12}$$

is constant and its components become eventually zero (i.e., only a finite number of components are non-zero). Furthermore, $C_{j,\alpha m_i\times m_i}\vec{a}$ for $a = 0, 1, \ldots, 2^{m_i} - 1$ and $j = 1, \ldots, s$ generate an order α digital (t, m_i, s)-

net over $\mathbb{F}_2$ (which is also an order α' digital (t, m_i, s)-net over $\mathbb{F}_2$ for $1 \le \alpha' \le \alpha$).

This means that the point set $\mathcal{P}_i$ is a digitally shifted order α digital (t, m_i, s)-net over $\mathbb{F}_2$ and the generating matrices

$$C_{1,\alpha m_i \times m_i}, \dots, C_{s,\alpha m_i \times m_i} \tag{13}$$

of this digital net are the left upper $\alpha m_i \times m_i$ submatrices of the generating matrices $C_1, \dots, C_s$ of the digital sequence. We denote the digital shift, which is given by (12), by $\boldsymbol{\sigma}_i$. Note that all the coordinates of the digital shift are dyadic rationals since the components of $\vec{\sigma}_{i,j}$ become eventually zero.

Let $\mathcal{D}_i$ denote the dual net corresponding to the digital net with generating matrices (13), i.e.,

$$\mathcal{D}_i = \{\boldsymbol{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s : C_{1,\alpha m_i \times m_i}^\top \vec{k}_1 + \cdots + C_{s,\alpha m_i \times m_i}^\top \vec{k}_s = \vec{0}\},$$

where for $k \in \mathbb{N}_0$ with base 2 expansion $k = \kappa_0 + \kappa_1 2 + \kappa_2 2^2 + \cdots$ we set $\vec{k} = (\kappa_0, \kappa_1, \dots, \kappa_{\alpha m_i - 1})^\top$. Set $\mathcal{D}_i^* = \mathcal{D}_i \setminus \{\boldsymbol{0}\}$.

We now obtain a bound on the $\mathcal{L}_2$ discrepancy using the dual nets $\mathcal{D}_i$.

For a vector $\boldsymbol{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ we put $\mu(\boldsymbol{k}) = \sum_{j=0}^s \mu(k_j)$, where, as already mentioned earlier, the function $\mu : \mathbb{N}_0 \to \mathbb{N}_0$ is defined by $\mu(0) = 0$ and for $k = \kappa_0 + \kappa_1 2 + \cdots + \kappa_{a-2} 2^{a-2} + 2^{a-1}$ with $\kappa_j \in \{0, 1\}$ by $\mu(k) = a$.

LEMMA 3.1. *Let $N = 2^{m_1} + \cdots + 2^{m_r}$ where $m_1 > \cdots > m_r \ge 0$. Using the notation above, let*

$$\mathcal{J}_{i,i'} = \{(\boldsymbol{k}, \boldsymbol{l}) \in \mathcal{D}_i^* \times \mathcal{D}_{i'}^* : r(\boldsymbol{k}, \boldsymbol{l}) \ne 0\}, \tag{14}$$

$$\mathcal{J}_{i,i'}(z) = \{(\boldsymbol{k}, \boldsymbol{l}) \in \mathcal{J}_{i,i'} : \mu(\boldsymbol{k}) + \mu(\boldsymbol{l}) = z\}. \tag{15}$$

Then

$$\mathcal{L}_{2,N}^2(\mathcal{S}_s) \ll_s \sum_{i,i'=1}^r \frac{2^{m_i}}{N} \frac{2^{m_{i'}}}{N} \sum_{z=m_i+m_{i'}-2t+2}^{\infty} \frac{|\mathcal{J}_{i,i'}(z)|}{2^z}. \tag{16}$$

Proof. By the character property (7) we have

$$\frac{1}{2^{m_i}} \sum_{n=2^{m_1}+\cdots+2^{m_i-1}}^{-1+2^{m_1}+\cdots+2^{m_i}} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) = \begin{cases} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{\sigma}_i) & \text{if } \boldsymbol{k} \in \mathcal{D}_i, \\ 0 & \text{if } \boldsymbol{k} \notin \mathcal{D}_i, \end{cases}$$

where again for $i = 1$ we set $2^{m_1} + \cdots + 2^{m_{i-1}} = 0$, and hence

$$\begin{aligned} \frac{1}{N} \sum_{n=0}^{N-1} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) &= \sum_{i=1}^r \frac{2^{m_i}}{N} \frac{1}{2^{m_i}} \sum_{n=2^{m_1}+\cdots+2^{m_i-1}}^{-1+2^{m_1}+\cdots+2^{m_i}} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x}_n) \\ &= \sum_{\substack{i=1 \\ \boldsymbol{k} \in \mathcal{D}_i}}^r \frac{2^{m_i}}{N} \mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{\sigma}_i). \end{aligned}$$

Inserting this into (11) and interchanging the order of summation we obtain

$$\mathcal{L}_{2,N}^2(\mathcal{S}_s) = \sum_{i,i'=1}^{r} \frac{2^{m_i}}{N}\frac{2^{m_{i'}}}{N} \sum_{(\boldsymbol{k},\boldsymbol{l})\in\mathcal{D}_i^*\times\mathcal{D}_{i'}^*} r(\boldsymbol{k},\boldsymbol{l})\,\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{\sigma}_i)\,\mathrm{wal}_{\boldsymbol{l}}(\boldsymbol{\sigma}_{i'}) \tag{17}$$

$$\le \sum_{i,i'=1}^{r} \frac{2^{m_i}}{N}\frac{2^{m_{i'}}}{N} \sum_{(\boldsymbol{k},\boldsymbol{l})\in\mathcal{J}_{i,i'}} |r(\boldsymbol{k},\boldsymbol{l})|,$$

since $|\mathrm{wal}_{\boldsymbol{k}}(\boldsymbol{x})| = 1$ for any $\boldsymbol{x}$.

According to the definition of $r(\boldsymbol{k},\boldsymbol{l})$ in Lemma 2.2 for $(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'}$ we have

$$|r(\boldsymbol{k},\boldsymbol{l})| \le \frac{1}{3^s 2^{\mu(\boldsymbol{k})+\mu(\boldsymbol{l})}}.$$

Thus from (17) we obtain

$$\mathcal{L}_{2,N}^2(\mathcal{S}_s) \ll_s \sum_{i,i'=1}^{r} \frac{2^{m_i}}{N}\frac{2^{m_{i'}}}{N} \sum_{(\boldsymbol{k},\boldsymbol{l})\in\mathcal{J}_{i,i'}} \frac{1}{2^{\mu(\boldsymbol{k})+\mu(\boldsymbol{l})}}. \tag{18}$$

Now we reorder the sum over all $(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'}$ according to the value of $\mu(\boldsymbol{k}) + \mu(\boldsymbol{l})$.

Assume that $\boldsymbol{k} = (k_1,\dots,k_s) \in \mathcal{D}_i^*$. Let $k_j = \kappa_{j,0} + \kappa_{j,1}2 + \cdots + \kappa_{j,a_j-2}2^{a_j-2} + 2^{a_j-1}$ with $a_j = \mu(k_j)$ for $j = 1,\dots,s$. Let further $\vec{c}_{j,u}$ denote the uth row vector of the matrix $C_{j,\alpha m_i\times m_i}$. Then

$$C_{1,\alpha m_i\times m_i}^{\top}\vec{k}_1 + \cdots + C_{s,\alpha m_i\times m_i}^{\top}\vec{k}_s = \vec{0}$$

is equivalent to

$$\sum_{j=1}^{s}\Big(\sum_{u=0}^{a_j-2}\vec{c}_{j,u+1}^{\,\top}\kappa_{j,u} + \vec{c}_{j,a_j-1}^{\,\top}\Big) = \vec{0}.$$

Hence it follows from the linear independence property for the row vectors of generating matrices of digital nets in Definition 1.5 that

$$\mu(\boldsymbol{k}) = a_1 + \cdots + a_s > m_i - t.$$

In the same way $\boldsymbol{l} \in \mathcal{D}_{i'}^*$ implies that $\mu(\boldsymbol{l}) > m_{i'} - t$. Hence $(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{D}_i^* \times \mathcal{D}_{i'}^*$ implies $\mu(\boldsymbol{k}) + \mu(\boldsymbol{l}) \ge m_i + m_{i'} - 2t + 2$.

Thus for the innermost sum in (18) we have

$$\sum_{(\boldsymbol{k},\boldsymbol{l})\in\mathcal{J}_{i,i'}} \frac{1}{2^{\mu(\boldsymbol{k})+\mu(\boldsymbol{l})}} = \sum_{z=m_i+m_{i'}-2t+2}^{\infty} \frac{|\mathcal{J}_{i,i'}(z)|}{2^z}.$$

By substituting this result into (18) the result follows. ∎

To obtain a bound on the right-hand side of (16), we first obtain a bound on the number of elements in the set $\mathcal{J}_{i,i'}(z)$. We do this in the next six lemmas.

LEMMA 3.2. *Using the notation above, we have*

$$|\mathcal{J}_{i,i'}(z)| = \sum_{z_1=m_i-t+1}^{z-m_{i'}+t-1} |\{(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'} : \mu(\boldsymbol{k}) = z_1 \text{ and } \mu(\boldsymbol{l}) = z-z_1\}|. \tag{19}$$

Proof. We have

$$|\mathcal{J}_{i,i'}(z)| = \sum_{z_1=0}^{z} |\{(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'} : \mu(\boldsymbol{k}) = z_1 \text{ and } \mu(\boldsymbol{l}) = z - z_1\}|.$$

Now $(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'}$ implies $\boldsymbol{k} \in \mathcal{D}_i^*$ and $\boldsymbol{l} \in \mathcal{D}_{i'}^*$. We already showed in the proof of Lemma 3.1 that $\boldsymbol{k} \in \mathcal{D}_i^*$ implies that $\mu(\boldsymbol{k}) > m_i - t$, and $\boldsymbol{l} \in \mathcal{D}_{i'}^*$ implies that $\mu(\boldsymbol{l}) > m_{i'} - t$. Thus we only need to consider the case where $z_1 > m_i - t$, and $z - z_1 > m_{i'} - t$, and hence the result follows. ∎

LEMMA 3.3. *Using the notation above, we have*

$$|\mathcal{J}_{i,i'}(z)| \le \sum_{z_1=m_i-t+1}^{z-m_{i'}+t-1} \min\Big\{ |\{\boldsymbol{k} \in \mathcal{D}_i^* : \mu(\boldsymbol{k}) = z_1\}| \max_{\substack{\boldsymbol{k}\in\mathcal{D}_i^* \\ \mu(\boldsymbol{k})=z_1}} |R_{i,i'}^{(1)}(\boldsymbol{k}, z-z_1)|,$$
$$|\{\boldsymbol{l} \in \mathcal{D}_{i'}^* : \mu(\boldsymbol{k}) = z - z_1\}| \max_{\substack{\boldsymbol{l}\in\mathcal{D}_{i'}^* \\ \mu(\boldsymbol{l})=z-z_1}} |R_{i,i'}^{(2)}(\boldsymbol{l}, z_1)| \Big\},$$

where

$$R_{i,i'}^{(1)}(\boldsymbol{k}, z-z_1) = \{\boldsymbol{l} \in \mathcal{D}_{i'}^* : (\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'}(z) \text{ and } \mu(\boldsymbol{l}) = z - z_1\},$$
$$R_{i,i'}^{(2)}(\boldsymbol{l}, z_1) = \{\boldsymbol{k} \in \mathcal{D}_i^* : (\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'}(z) \text{ and } \mu(\boldsymbol{k}) = z_1\}.$$

Proof. Each summand in (19) can be estimated on the one hand by

$$|\{(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'} : \mu(\boldsymbol{k}) = z_1 \quad \text{and} \quad \mu(\boldsymbol{l}) = z - z_1\}|$$
$$\le |\{\boldsymbol{k} \in \mathcal{D}_i^* : \mu(\boldsymbol{k}) = z_1\}| \max_{\substack{\boldsymbol{k}\in\mathcal{D}_i^* \\ \mu(\boldsymbol{k})=z_1}} |R_{i,i'}^{(1)}(\boldsymbol{k}, z-z_1)|,$$

and on the other hand by

$$|\{(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'} : \mu(\boldsymbol{k}) = z_1 \quad \text{and} \quad \mu(\boldsymbol{l}) = z - z_1\}|$$
$$\le |\{\boldsymbol{l} \in \mathcal{D}_{i'}^* : \mu(\boldsymbol{k}) = z - z_1\}| \max_{\substack{\boldsymbol{l}\in\mathcal{D}_{i'}^* \\ \mu(\boldsymbol{l})=z-z_1}} |R_{i,i'}^{(2)}(\boldsymbol{l}, z_1)|.$$

Hence the result follows. ∎

To prove the next results we introduce some notation. Let $k_j, l_j \in \mathbb{N}_0$. In the following we simultaneously use two different notations for the binary expansion of k_j and l_j. First let

$$k_j = 2^{a_{j,1}-1} + \cdots + 2^{a_{j,\widetilde{v}_j}-1}$$

with $a_{j,1} > \cdots > a_{j,\widetilde{v}_j} > 0$ and

$$l_j = 2^{b_{j,1}-1} + \cdots + 2^{b_{j,\widetilde{w}_j}-1}$$

with $b_{j,1} > \cdots > b_{j,\widetilde{w}_j} > 0$. Thus $\widetilde{v}_j$ denotes the number of non-zero digits of k_j, and $\widetilde{w}_j$ denotes the number of non-zero digits of l_j. For $k_j = 0$ we use the convention that $\widetilde{v}_j = 0$ and $a_{j,1} = 0$. Further we set $a_{j,\widetilde{v}_j+i} = b_{j,\widetilde{w}_j+i} = 0$ for $i > 0$.

We also use the notation

$$k_j = k_{j,0} + k_{j,1}2 + \cdots + k_{j,a_{j,1}-1}2^{a_{j,1}-1}$$

with binary digits $k_{j,i} \in \{0,1\}$. Thus

$$k_{j,i} = \begin{cases} 1 & \text{if } i = a_{j,v} \text{ for some } 1 \le v \le \widetilde{v}_j, \\ 0 & \text{otherwise.} \end{cases}$$

Analogously we write

$$l_j = l_{j,0} + l_{j,1}2 + \cdots + l_{j,b_{j,1}-1}2^{b_{j,1}-1}$$

with binary digits $l_{j,i} \in \{0,1\}$. Thus

$$l_{j,i} = \begin{cases} 1 & \text{if } i = b_{j,w} \text{ for some } 1 \le w \le \widetilde{w}_j, \\ 0 & \text{otherwise.} \end{cases}$$

We now study the factors appearing in the bound in Lemma 3.3 separately in two steps.

LEMMA 3.4. *For $z_1 \ge m_i - t + 1$ we have*

$$|\{\boldsymbol{k} \in \mathcal{D}_i^* : \mu(\boldsymbol{k}) = z_1\}| \ll_s \binom{z_1 + s - 1}{s-1} 2^{z_1 - m_i + t - 1},$$

and for $z - z_1 \ge m_{i'} - t + 1$ we have

$$|\{\boldsymbol{l} \in \mathcal{D}_{i'}^* : \mu(\boldsymbol{l}) = z - z_1\}| \ll_s \binom{z - z_1 + s - 1}{s-1} 2^{z - z_1 - m_{i'} + t - 1}.$$

Proof. It suffices to show the first estimate, the second estimate is a direct consequence of the first bound. The number of $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathcal{D}_i^*$ with $\mu(\boldsymbol{k}) = z_1$ has been studied in [14]. Assume first that $k_j > 0$ for $1 \le j \le s$. The case where one or more of the k_j's are zero follows by the same arguments. Let $\Sigma(v_1, \ldots, v_s)$ denote the number of such $\boldsymbol{k} = (k_1, \ldots, k_s) \in \mathcal{D}_i^*$

with $\mu(k_j) = a_{j,1} = v_j$. Then $\boldsymbol{k} \in \mathcal{D}_i^*$ implies that

$$\begin{aligned}(20)\qquad &\vec{c}_{1,1}^{\,\top} k_{1,0} + \cdots + \vec{c}_{1,v_1-1}^{\,\top} k_{1,v_1-2} + \vec{c}_{1,v_1}^{\,\top} \\ &+ \vec{c}_{2,1}^{\,\top} k_{2,0} + \cdots + \vec{c}_{2,v_2-1}^{\,\top} k_{2,v_2-2} + \vec{c}_{2,v_2}^{\,\top} \\ &\vdots \\ &+ \vec{c}_{s,1}^{\,\top} k_{s,0} + \cdots + \vec{c}_{s,v_s-1}^{\,\top} k_{s,v_s-2} + \vec{c}_{s,v_s}^{\,\top} = \vec{0},\end{aligned}$$

where $\vec{c}_{j,u} \in \mathbb{F}_2^{m_i}$ denotes the uth row vector of the matrix $C_{j,\alpha m_i \times m_i}$. Since by the (order 1) digital (t, m_i, s)-net property the vectors

$$\vec{c}_{1,1}, \ldots, \vec{c}_{1,v_1}, \ldots, \vec{c}_{s,1}, \ldots, \vec{c}_{s,v_s}$$

are linearly independent as long as $v_1 + \cdots + v_s \le m_i - t$, we must have

$$(21)\qquad v_1 + \cdots + v_s \ge m_i - t + 1.$$

Let now A denote the $m_i \times ((v_1 - 1) + \cdots + (v_s - 1))$ matrix with column vectors $\vec{c}_{1,1}^{\,\top}, \ldots, \vec{c}_{1,v_1-1}^{\,\top}, \ldots, \vec{c}_{s,1}^{\,\top}, \ldots, \vec{c}_{s,v_s-1}^{\,\top}$, i.e.,

$$A := (\vec{c}_{1,1}^{\,\top}, \ldots, \vec{c}_{1,v_1-1}^{\,\top}, \ldots, \vec{c}_{s,1}^{\,\top}, \ldots, \vec{c}_{s,v_s-1}^{\,\top}).$$

Further let

$$\vec{f} := \vec{c}_{1,v_1}^{\,\top} + \cdots + \vec{c}_{s,v_s}^{\,\top}$$

and

$$\vec{k} := \underbrace{(k_{1,0}, \ldots, k_{1,v_1-2}, \ldots, k_{s,0}, \ldots, k_{s,v_s-2})^{\top}}_{\text{length } (v_1-1)+\cdots+(v_s-1)}.$$

Then the linear system of equations (20) can be written as

$$(22)\qquad A\vec{k} = \vec{f}$$

and hence

$$\Sigma(v_1, \ldots, v_s) = \sum_{\substack{\vec{k} \in \mathbb{F}_2^{(v_1-1)+\cdots+(v_s-1)} \\ A\vec{k} = \vec{f}}} 1 = |\{\vec{k} \in \mathbb{F}_2^{(v_1-1)+\cdots+(v_s-1)} : A\vec{k} = \vec{f}\}|.$$

By the definition of the matrix A and since $C_{1,\alpha m_i \times m_i}, \ldots, C_{s,\alpha m_i \times m_i}$ are the generating matrices of an (order 1) digital (t, m_i, s)-net over $\mathbb{F}_2$ we have

$$\operatorname{rank}(A) \begin{cases} = (v_1 - 1) + \cdots + (v_s - 1) & \text{if } (v_1 - 1) + \cdots + (v_s - 1) \le m_i - t, \\ \ge m_i - t & \text{otherwise.} \end{cases}$$

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

$$\dim(L) \begin{cases} = 0 & \text{if } v_1 + \cdots + v_s \le m_i - t + s, \\ \le v_1 + \cdots + v_s - m_i + t - s & \text{otherwise.} \end{cases}$$

Hence if $v_1 + \cdots + v_s \le m_i - t + s$ we find that the system (22) has at most one solution and if $v_1 + \cdots + v_s > m_i - t + s$ then the system (22) has at most $2^{v_1+\cdots+v_s-m_i+t-s}$ solutions, i.e.,

$$\Sigma(v_1,\ldots,v_s) \le \begin{cases} 1 & \text{if } v_1 + \cdots + v_s \le m_i - t + s, \\ 2^{v_1+\cdots+v_s-m_i+t-s} & \text{if } v_1 + \cdots + v_s > m_i - t + s. \end{cases}$$

Recall that $v_1 + \cdots + v_s = \mu(\boldsymbol{k})$.

In the following let $\binom{n}{k}$ denote the binomial coefficient, where we set $\binom{n}{k} = 0$ if $k > n$. Thus

$$|\{\boldsymbol{k} \in \mathcal{D}_i^* : k_j > 0 \text{ for } j = 1,\ldots,s \text{ and } \mu(\boldsymbol{k}) = z_1\}| = \begin{cases} \binom{z_1+s-1}{s-1} & \text{if } z_1 \le m_i - t + s, \\ \binom{z_1+s-1}{s-1} 2^{z_1-m_i+t-s} & \text{if } z_1 > m_i - t + s. \end{cases}$$

In general, for $\emptyset \ne u \subseteq \{1,\ldots,s\}$ we have

$$|\{\boldsymbol{k} \in \mathcal{D}_i^* : k_j > 0 \text{ for } j \in u,\ k_j = 0 \text{ otherwise, and } \mu(\boldsymbol{k}) = z_1\}| = \begin{cases} \binom{z_1+|u|-1}{|u|-1} & \text{if } z_1 \le m_i - t + |u|, \\ \binom{z_1+|u|-1}{|u|-1} 2^{z_1-m_i+t-|u|} & \text{if } z_1 > m_i - t + |u|. \end{cases}$$

Thus, in general, for $z_1 \ge m_i - t + 1$ we have

$$|\{\boldsymbol{k} \in \mathcal{D}_i^* : \mu(\boldsymbol{k}) = z_1\}| \ll_s \binom{z_1+s-1}{s-1} 2^{z_1-m_i+t-1}. \ \blacksquare$$

LEMMA 3.5. *Let $R^{(1)}_{i,i'}(\boldsymbol{k}, z - z_1)$ and $R^{(2)}_{i,i'}(\boldsymbol{l}, z_1)$ be defined as in Lemma 3.3. Then for $\boldsymbol{k} \in \mathcal{D}_i^*$ we have*

$$|R^{(1)}_{i,i'}(\boldsymbol{k}, z - z_1)| \le \binom{2(z-z_1) - 2m_{i'} + t + s}{s} \binom{3(z-z_1) - 3m_{i'} + t + s}{s},$$

and for $\boldsymbol{l} \in \mathcal{D}_{i'}^*$ we have

$$|R^{(2)}_{i,i'}(\boldsymbol{l}, z_1)| \le \binom{2z_1 - 2m_i + t + s}{s} \binom{3z_1 - 3m_i + t + s}{s}.$$

Proof. Again it suffices to show the first estimate, the second estimate follows by the same arguments. For the proof we first need to analyze for which $(\boldsymbol{k}, \boldsymbol{l}) \in \mathcal{D}_i \times \mathcal{D}_{i'}$ the factors $r(\boldsymbol{k}, \boldsymbol{l})$ are different from 0. To do so we consider a number of cases.

Recall that $r(\boldsymbol{k},\boldsymbol{l}) = \prod_{j=1}^{s} r(k_j,l_j)$. For $r(k_j,l_j) \neq 0$ it follows that in some sense k_j and l_j cannot be too different. Let us elaborate this in more detail: Assume that $r(k_j,l_j) \neq 0$. Now Lemma 2.2 implies that in order for $r(k_j,l_j)$ not to be 0 we must have $0 \leq |\widetilde{v}_j - \widetilde{w}_j| \leq 2$. Further we must have:

(i) $|\widetilde{v}_j - \widetilde{w}_j| = 0 \;\Rightarrow\; a_{j,2} = b_{j,2}, \ldots, a_{j,\widetilde{v}_j} = b_{j,\widetilde{v}_j}$,
(ii) $|\widetilde{v}_j - \widetilde{w}_j| = 1 \;\Rightarrow\; k_j = 0$ or $l_j = 0$,
(iii) $|\widetilde{v}_j - \widetilde{w}_j| = 2 \;\Rightarrow\;$ if $\widetilde{v}_j = \widetilde{w}_j + 2$ then $a_{j,3} = b_{j,1}, \ldots, a_{j,\widetilde{v}_j} = b_{j,\widetilde{w}_j}$,
if $\widetilde{w}_j = \widetilde{v}_j + 2$ then $b_{j,3} = a_{j,1}, \ldots, b_{j,\widetilde{w}_j} = a_{j,\widetilde{v}_j}$.

If $|\widetilde{v}_j - \widetilde{w}_j| > 2$ we always have $r(k_j,l_j) = 0$.

For given $(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}_{i,i'}(z)$ we define the following sets for $-2 \leq \tau \leq 2$:

$$\alpha_\tau = \{j \in \{1,\ldots,s\} : \widetilde{v}_j = \widetilde{w}_j + \tau\}.$$

Note that $\alpha_\tau \cap \alpha_{\tau'} = \emptyset$ for $\tau \neq \tau'$ and $\bigcup_{\tau=-2}^{2} \alpha_\tau = \{1,\ldots,s\}$ by Lemma 2.2. We observe that:

(1) For $j \in \alpha_2$ we have $l_{j,i} = k_{j,i}$ for $0 \leq i < a_{j,2} - 1$.
(2) For $j \in \alpha_1$ we have $l_j = 0$ and $k_j = 2^{a_{j,1}-1}$.
(3) For $j \in \alpha_0$ we have $k_{j,i} = l_{j,i}$ for $0 \leq i < \min\{a_{j,1}, b_{j,1}\} - 1$.
(4) For $j \in \alpha_{-1}$ we have $l_j = 2^{b_{j,1}-1}$ and $k_j = 0$.
(5) For $j \in \alpha_{-2}$ we have $l_{j,i} = k_{j,i}$ for $0 \leq i < b_{j,2} - 1$.

Thus, in all cases, $k_{j,i} = l_{j,i}$ for $0 \leq i < \min\{a_{j,2} - 1, b_{j,2} - 1\}$. We now set

$$h_{j,i} = k_{j,i} = l_{j,i} \quad \text{for all } 1 \leq j \leq s \text{ and } 0 \leq i < \min\{a_{j,2} - 1, b_{j,2} - 1\},$$

and for $u_j = \min\{a_{j,2} - 1, b_{j,2} - 1\}$ we set

$$h_j = h_{j,0} + h_{j,1}2 + \cdots + h_{j,u_j-1}2^{u_j-1} \quad \text{for } 1 \leq j \leq s$$

if $u_j > 0$ and $h_j = 0$ otherwise. Thus we only need to consider the cases where

$$k_j = h_j + \lfloor 2^{a_{j,2}-1} \rfloor + \lfloor 2^{a_{j,1}-1} \rfloor, \qquad l_j = h_j + \lfloor 2^{b_{j,2}-1} \rfloor + \lfloor 2^{b_{j,1}-1} \rfloor$$

for $1 \leq j \leq s$.

We now prove a bound on $|R^{(1)}_{i,i'}(\boldsymbol{k}, z - z_1)|$. Let $\vec{c}_{j,u}$ denote the uth row of the matrix $C_{j,\alpha m_{i'} \times m_{i'}}$.

Let $\boldsymbol{k} \in \mathcal{D}^*_i$ be fixed and $\mu(k_j) = a_{j,1}$ for $1 \leq j \leq s$. We have $|\widetilde{v}_j - \widetilde{w}_j| \leq 2$ and $\boldsymbol{l} \in \mathcal{D}^*_{i'}$ implies that

$$\begin{aligned}
&\vec{c}_{1,1}^{\top} h_{1,0} + \cdots + \vec{c}_{1,b_{1,2}-1}^{\top} h_{1,b_{1,2}-2} + \vec{c}_{1,b_{1,2}}^{\top} + \vec{c}_{1,b_{1,1}}^{\top} \\
&+ \vec{c}_{2,1}^{\top} h_{2,0} + \cdots + \vec{c}_{2,b_{2,2}-1}^{\top} h_{2,b_{2,2}-2} + \vec{c}_{2,b_{2,2}}^{\top} + \vec{c}_{2,b_{2,1}}^{\top} \\
&\vdots \\
&+ \vec{c}_{s,1}^{\top} h_{s,0} + \cdots + \vec{c}_{s,b_{s,2}-1}^{\top} h_{s,b_{s,2}-2} + \vec{c}_{s,b_{s,2}}^{\top} + \vec{c}_{s,b_{s,1}}^{\top} = \vec{0}.
\end{aligned}$$

If $b_{j,1}$ or $b_{j,2}$ is zero, we set $\vec{c}_{j,0}^{\,\top} = \vec{0}$. Note that we consider $\boldsymbol{k}$ to be fixed, thus the $h_{j,i}$'s are also fixed. For $j \in \alpha_1 \cup \alpha_2$ the values $b_{j,1}, b_{j,2}$ are fixed by k_j as shown in cases (1) and (2) above. For $j \in \alpha_0 \cup \alpha_{-1}$ the values $b_{j,2}$ are fixed by the choice of k_j but $b_{j,1}$ is not; see cases (3) and (4). For $j \in \alpha_{-2}$ neither $b_{j,1}$ nor $b_{j,2}$ is fixed. Thus it follows that

$$\sum_{j\in\alpha_0} \vec{c}_{j,b_{j,1}}^{\,\top} + \sum_{j\in\alpha_{-1}} \vec{c}_{j,b_{j,1}}^{\,\top} + \sum_{j\in\alpha_{-2}} (\vec{c}_{j,b_{j,2}}^{\,\top} + \vec{c}_{j,b_{j,1}}^{\,\top}) = \sum_{j=1}^{s} \sum_{r=0}^{b_{j,2}-2} \vec{c}_{j,r+1}^{\,\top} h_{j,r} + \sum_{j\in\alpha_1\cup\alpha_2} \vec{c}_{j,b_{j,2}}^{\,\top} =: \vec{c}^{\,\top},$$

where the vector $\vec{c}^{\top}$ is fixed by $\boldsymbol{k}$, since the $h_{i,j}$ and $b_{j,1}, b_{j,2}$ are fixed by $\boldsymbol{k}$ for $j \in \alpha_1 \cup \alpha_2$. Since $\mu(l_j) = b_{j,1}$ for $1 \le j \le s$ we have $b_{1,1} + \cdots + b_{s,1} = z - z_1 =: z_2$.

Since h_j is fixed by k_j for $1 \le j \le s$, it follows that for each given vector $(b_{j,i})_{1\le i\le 2, 1\le j\le s}$, where $b_{j,1} > b_{j,2}$ and where $b_{1,1}+\cdots+b_{s,1} = z_2$, at most one such solution exists. Thus $|R^{(1)}_{i,i'}(\boldsymbol{k}, z_2)|$ is bounded by the number of possible choices of $(b_{j,i})_{1\le i\le 2,1\le j\le s}$, for which we prove a bound in the following.

The order 2 and order 1 digital (t, m_i, s)-net property and $\boldsymbol{l} \in \mathcal{D}^*_{i'}$ imply that

$$b_{1,1} + b_{1,2} + b_{2,1} + b_{2,2} + \cdots + b_{s,1} + b_{s,2} > 2m_{i'} - t,$$
$$z_2 = b_{1,1} + b_{2,1} + \cdots + b_{s,1} > m_{i'} - t.$$

Thus we have

$$b_{1,2} + \cdots + b_{s,2} \ge 2m_{i'} - t - z_2 + 1.$$

Let $b_{j,1} = \delta_j + b_{j,2}$, thus $\delta_j \ge 0$ (where $\delta_j = 0$ if $l_j = 0$). Then

$$z_2 = b_{1,1} + \cdots + b_{s,1} = \delta_1 + \cdots + \delta_s + b_{1,2} + \cdots + b_{s,2}$$
$$\ge \delta_1 + \cdots + \delta_s + 2m_{i'} - t - z_2 + 1.$$

and therefore

$$\delta_1 + \cdots + \delta_s \le 2z_2 - 2m_{i'} + t.$$

Thus, for given $b_{1,2}, \ldots, b_{s,2}$, the number of possible choices of $b_{1,1}, \ldots, b_{s,1}$ with $b_{1,1} + \cdots + b_{s,1} = z_2$ is bounded by the number of possible choices of $\delta_1, \ldots, \delta_s$, which itself is bounded from above by

$$\sum_{r=0}^{2z_2-2m_{i'}+t} \binom{r+s-1}{s-1} = \binom{2z_2 - 2m_{i'} + t + s}{s}.$$

Now consider the number of possible choices of $(b_{j,2})_{1\le j\le s}$. If $j \in \bigcup_{\tau=-1}^{2} \alpha_\tau$, then $b_{j,2}$ is fixed since k_j is fixed, and if $j \in \alpha_{-2}$, then $b_{j,1} > b_{j,2} > b_{j,3} = a_{j,1}$. Note that $b_{j,3}$ is fixed since k_j is fixed for all $1 \le j \le s$. By

the order 3, order 2 and order 1 digital net property and $\boldsymbol{l} \in \mathcal{D}^*_{i'}$ we have

$$b_{1,1} + b_{1,2} + b_{1,3} + \cdots + b_{s,1} + b_{s,2} + b_{s,3} > 3m_{i'} - t,$$
$$b_{1,1} + b_{1,2} + \cdots + b_{s,1} + b_{s,2} > 2m_{i'} - t,$$
$$z_2 = b_{1,1} + \cdots + b_{s,1} > m_{i'} - t.$$

Let $z_2' = b_{1,2} + b_{2,2} + \cdots + b_{s,2} < z_2$. Then

$$b_{1,3} + \cdots + b_{s,3} > 3m_{i'} - t - z_2 - z_2' > 3m_{i'} - t - 2z_2.$$

Let $b_{j,2} = \delta_j' + b_{j,3}$. Then $\delta_j' \geq 0$. Then we have

$$z_2 > b_{1,2} + \cdots + b_{s,2} = \delta_1' + \cdots + \delta_s' + b_{1,3} + \cdots + b_{s,3}$$
$$\geq \delta_1' + \cdots + \delta_s' + 3m_{i'} - t - 2z_2 + 1$$

and therefore

$$\delta_1' + \cdots + \delta_s' \leq 3z_2 - 3m_{i'} + t - 1.$$

Since $b_{1,3}, \ldots, b_{s,3}$ are fixed, the number of admissible $b_{1,2}, \ldots, b_{s,2}$ is bounded from above by the number of possible choices of $\delta_1', \ldots, \delta_s'$, which in turn is bounded by

$$\sum_{r=0}^{3z_2-3m_{i'}+t} \binom{r+s-1}{s-1} = \binom{3z_2 - 3m_{i'} + t + s}{s}.$$

Since the number of possible choices of $(b_{j,i})_{1\leq i\leq 2, 1\leq j\leq s}$ is bounded by the product of the number of possible choices of $b_{1,1}, \ldots, b_{s,1}$ and the number of possible choices of $b_{1,2}, \ldots, b_{s,2}$, we deduce

$$|R^{(1)}_{i,i'}(\boldsymbol{k}, z_2)| \leq \binom{2z_2 - 2m_{i'} + t + s}{s} \binom{3z_2 - 3m_{i'} + t + s}{s}.$$

Thus the statement of the lemma follows. ∎

Before we combine Lemmas 3.4 and 3.5 to obtain a bound on $|\mathcal{J}_{i,i'}(z)|$, we show in the next lemma that for 'small' z the set $\mathcal{J}_{i,i'}(z)$ is empty. In the proof we need to assume that $\alpha \geq 5$.

LEMMA 3.6. *Let $\alpha \geq 5$. Then $\mathcal{J}_{i,i'}(z) = \emptyset$ if $z < \frac{1}{4}\max\{5m_i + 3m_{i'}, 3m_i + 5m_{i'}\} - t + \frac{3}{4}$.*

Proof. We use the notation from the proof of Lemma 3.5.

Assume that $(\boldsymbol{k}, \boldsymbol{l}) \in \mathcal{J}_{i,i'}(z)$. Consider again the five cases from that proof. The following hold:

(1) For $j \in \alpha_2$ we have $a_{j,i+2} = b_{j,i}$ for $i = 1, \ldots, \widetilde{w}_j$ and $\widetilde{w}_j = \widetilde{v}_j - 2$.
(2) For $j \in \alpha_1$ we have $a_{j,i+1} = b_{j,i} = 0$ for $i = 1, \ldots, \widetilde{w}_j$ and $\widetilde{w}_j = \widetilde{v}_j - 1$.
(3) For $j \in \alpha_0$ we have $a_{j,i+1} = b_{j,i+1}$ for $i = 1, \ldots, \widetilde{w}_j$ and $\widetilde{w}_j = \widetilde{v}_j$.
(4) For $j \in \alpha_{-1}$ we have $a_{j,i} = b_{j,i+1} = 0$ for $i = 1, \ldots, \widetilde{v}_j$ and $\widetilde{v}_j = \widetilde{w}_j - 1$.
(5) For $j \in \alpha_{-2}$ we have $a_{j,i} = b_{j,i+2}$ for $i = 1, \ldots, \widetilde{v}_j$ and $\widetilde{v}_j = \widetilde{w}_j - 2$.

Since $a_{j,i} > a_{j,i+1}$ we therefore have $b_{j,3} \geq a_{j,5}$ for $1 \leq j \leq s$. By the order 5 digital (t,m,s)-net property we have

$$a_{1,1}+a_{1,2}+a_{1,3}+a_{1,4}+a_{1,5}+\cdots+a_{s,1}+a_{s,2}+a_{s,3}+a_{s,4}+a_{s,5} > 5m_i - t$$

and

$$\begin{aligned} z_1 = a_{1,1}+\cdots+a_{s,1} &\geq a_{1,2}+\cdots+a_{s,2} \\ &\geq a_{1,3}+\cdots+a_{s,3} \geq a_{1,4}+\cdots+a_{s,4} \end{aligned}$$

Thus, since $b_{j,i} > b_{j,i+1}$, we obtain

$$z - z_1 = z_2 = b_{1,1}+\cdots+b_{s,1} \geq b_{1,3}+\cdots+b_{s,3} \geq a_{1,5}+\cdots+a_{s,5} \geq 5m_i - t - 4z_1.$$

From the proof of Lemma 3.2 we have $z - z_1 \geq m_{i'} - t + 1$, therefore

$$z \geq 5m_i - t - 3z_1 \geq 5m_i - t + 3(m_{i'} - t + 1 - z),$$

which implies

$$z \geq \frac{5m_i + 3m_{i'}}{4} - t + \frac{3}{4}.$$

Analogously we have

$$z \geq \frac{3m_i + 5m_{i'}}{4} - t + \frac{3}{4}.$$

Thus we have $\mathcal{J}_{i,i'}(z) = \emptyset$ if $z < \frac{1}{4}\max\{5m_i + 3m_{i'}, 3m_i + 5m_{i'}\} - t + \frac{3}{4}$. ∎

In the following we obtain a bound on $|\mathcal{J}_{i,i'}(z)|$ for $z \geq m_i + m_{i'} - 2t + 2$. In Lemma 3.6 we considered $z < \frac{1}{4}\max\{5m_i + 3m_{i'}, 3m_i + 5m_{i'}\} - t + \frac{3}{4}$. At the beginning of this section we showed that $t \geq 3$. Since $\frac{1}{4}\max\{5m_i + 3m_{i'}, 3m_i + 5m_{i'}\} - t + \frac{3}{4} \geq m_i + m_{i'} - 2t + 2$ for $t \geq 3$, Lemmas 3.6 and 3.7 yield a bound on $|\mathcal{J}_{i,i'}(z)|$ for all $z \geq 0$.

LEMMA 3.7. *For all $\kappa \geq 0$ we have*

$$\begin{aligned} &|\mathcal{J}_{i,i'}(m_i + m_{i'} - 2t + 2 + \kappa)| \\ &\qquad \leq 2^{\kappa/2+2} \sum_{z_1'=0}^{\lceil \kappa/2 \rceil} \binom{z_1' + m_i - t + s}{s-1} \\ &\qquad\quad \times \binom{2(\kappa - z_1') + s + 2 - t}{s} \binom{3(\kappa - z_1') + s + 3 - 2t}{s}. \end{aligned}$$

Proof. Combining Lemmas 3.3–3.5 we obtain

$$
\begin{aligned}
&|\mathcal{J}_{i,i'}(z)| \\
&\quad\le \sum_{z_1=m_i-t+1}^{z-m_{i'}+t-1} \min\Bigg\{ 2^{z_1-m_i+t-1}\binom{z_1+s-1}{s-1}\binom{2z-2z_1-2m_{i'}+t+s}{s} \\
&\qquad\qquad \times \binom{3z-3z_1-3m_{i'}+t+s}{s}, \\
&\qquad 2^{z-z_1-m_{i'}+t-1}\binom{z-z_1+s-1}{s-1}\binom{2z_1-2m_i+t+s}{s} \\
&\qquad\qquad \times \binom{3z_1-3m_i+t+s}{s}\Bigg\}.
\end{aligned}
$$

To simplify this bound further we first use the change of variable $z = m_i + m_{i'} - 2t + 2 + \kappa$ for $\kappa \ge 0$. Then we have

$$
\begin{aligned}
&|\mathcal{J}_{i,i'}(m_i + m_{i'} - 2t + 2 + \kappa)| \\
&\qquad\le \sum_{z_1'=0}^{\kappa} \min\Bigg\{ 2^{z_1'}\binom{z_1'+m_i-t+s}{s-1}\binom{2(\kappa-z_1')+s+2-t}{s} \\
&\qquad\qquad \times \binom{3(\kappa-z_1')+s+3-2t}{s}, \\
&\qquad 2^{\kappa-z_1'}\binom{\kappa-z_1'+m_{i'}-t+s}{s-1}\binom{2z_1'+s+2-t}{s}\binom{3z_1'+s+3-2t}{s}\Bigg\}.
\end{aligned}
$$

Let

$$
B(z_1', z_2') = 2^{z_1'}\binom{z_1'+m_i-t+s}{s-1}\binom{2z_2'+s+2-t}{s}\binom{3z_2'+s+3-2t}{s}.
$$

Then we obtain

$$
\begin{aligned}
(23)\qquad |\mathcal{J}_{i,i'}(m_i+m_{i'}-2t+2+\kappa)| &\le \sum_{z_1'=0}^{\kappa} \min\{B(z_1', \kappa-z_1'), B(\kappa-z_1', z_1')\} \\
&\le 2\sum_{z_1'=0}^{\lceil\kappa/2\rceil} \min\{B(z_1', \kappa-z_1'), B(\kappa-z_1', z_1')\} \le 2\sum_{z_1'=0}^{\lceil\kappa/2\rceil} B(z_1', \kappa-z_1') \\
&\le 2^{\kappa/2+2}\sum_{z_1'=0}^{\lceil\kappa/2\rceil} \binom{z_1'+m_i-t+s}{s-1}\binom{2(\kappa-z_1')+s+2-t}{s} \\
&\qquad \times \binom{3(\kappa-z_1')+s+3-2t}{s}. \ \blacksquare
\end{aligned}
$$

The following lemma now implies Theorem 1.1. Since the proof makes use of Lemma 3.6 we need to assume that $\alpha \geq 5$.

LEMMA 3.8. *Let $\alpha \geq 5$. Let $N = 2^{m_1} + \cdots + 2^{m_r} \geq 2$ with $m_1 > \cdots > m_r \geq 0$. Then*

$$\mathcal{L}_{2,N}^2(\mathcal{S}_s) \ll_s \frac{(\log N)^{s-1}}{N^2} r.$$

Proof. Assume that $i \leq i'$. Note that for $\kappa < \lfloor (m_i - m_{i'})/4 + t - 5/4 \rfloor$ we have $\mathcal{J}_{i,i'}(m_i + m_{i'} - 2t + 2 + \kappa) = \emptyset$ by Lemma 3.6. Now we use Lemma 3.7 to deduce for the innermost sum in Lemma 3.1 that

$$\begin{aligned}
&\sum_{z=m_i+m_{i'}-2t+2}^{\infty} \frac{|\mathcal{J}_{i,i'}(z)|}{2^z} \\
&\quad \ll_s \frac{1}{2^{m_i+m_{i'}}} \sum_{\kappa=\lfloor (m_i-m_{i'})/4+t-5/4 \rfloor}^{\infty} \frac{|\mathcal{J}_{i,i'}(m_i+m_{i'}-2t+2+\kappa)|}{2^\kappa} \\
&\quad \ll_s \frac{1}{2^{m_i+m_{i'}}} \sum_{\kappa=\lfloor (m_i-m_{i'})/4+t-5/4 \rfloor}^{\infty} \frac{2^2}{2^{\kappa/2}} \sum_{z_1'=0}^{\lceil \kappa/2 \rceil} \binom{z_1' + m_i - t + s}{s-1} \\
&\qquad \times \binom{2(\kappa - z_1') + s + 2 - t}{s} \binom{3(\kappa - z_1') + s + 3 - 2t}{s}.
\end{aligned}$$

Since t depends only on the dimension s but not on $m_i, m_{i'}$, we can simplify the above expression to obtain

$$\begin{aligned}
&\sum_{z=m_i+m_{i'}-2t+2}^{\infty} \frac{|\mathcal{J}_{i,i'}(z)|}{2^z} \\
&\quad \ll_s \frac{1}{2^{m_i+m_{i'}}} \sum_{\kappa=\lfloor (m_i-m_{i'})/4 \rfloor}^{\infty} \frac{1}{2^{\kappa/2}} \sum_{z_1'=0}^{\lceil \kappa/2 \rceil} \binom{z_1' + m_i}{s-1} \binom{2(\kappa - z_1')}{s} \binom{3(\kappa - z_1')}{s}.
\end{aligned}$$

We estimate the binomial coefficients using $0 \leq z_1' \leq \kappa$ to obtain

$$\binom{z_1' + m_i}{s-1} \ll_s (m_i+1)^{s-1}(z_1'+1)^{s-1} \ll_s (\log N)^{s-1}(\kappa+1)^{s-1}$$

and

$$\binom{2(\kappa - z_1')}{s} \binom{3(\kappa - z_1')}{s} \ll_s (\kappa+1)^{2s}.$$

Thus we have

$$\sum_{z=m_i+m_{i'}-2t+2}^{\infty} \frac{|\mathcal{J}_{i,i'}(z)|}{2^z} \ll_s \frac{(\log N)^{s-1}}{2^{m_i+m_{i'}}} \sum_{\kappa=\lfloor (m_i-m_{i'})/4 \rfloor}^{\infty} \frac{(\kappa+1)^{3s}}{2^{\kappa/2}}.$$

Inserting this bound into Lemma 3.1 we obtain

$$\mathcal{L}_{2,N}^2(\mathcal{S}_s) \ll_s \frac{(\log N)^{s-1}}{N^2} \sum_{1\le i\le i'\le r} \sum_{\kappa=\lfloor (m_i-m_{i'})/4\rfloor}^{\infty} \frac{(\kappa+1)^{3s}}{2^{\kappa/2}}.$$

Using the fact that for $i \le i'$ we have $m_i \ge m_{i'}$ we deduce for any fixed $1 \le i \le r$ that

$$\begin{aligned}\sum_{i'=i}^{r} \sum_{\kappa=\lfloor (m_i-m_{i'})/4\rfloor}^{\infty} \frac{(\kappa+1)^{3s}}{2^{\kappa/2}} &\ll_s \sum_{i'=i}^{r} \sum_{\kappa=\lfloor (m_i-m_{i'})/4\rfloor}^{\infty} \frac{1}{2^{\kappa/4}} \\ &\ll \sum_{i'=i}^{r} \frac{1}{2^{(m_i-m_{i'})/16}} \le \sum_{q=0}^{\infty} \frac{1}{2^{q/16}} \ll 1.\end{aligned}$$

Thus we obtain

$$\sum_{1\le i\le i'\le r} \sum_{\kappa=\lfloor (m_i-m_{i'})/4\rfloor}^{\infty} \frac{(\kappa+1)^{3s}}{2^{\kappa/2}} \ll_s r$$

and therefore

$$\mathcal{L}_{2,N}^2(\mathcal{S}_s) \ll_s \frac{(\log N)^{s-1}}{N^2} r,$$

where $r = S(N)$ denotes the number of non-zero digits in the binary expansion of N. ∎

4. The proof of Corollary 1.3. We first prove a bound on the $\mathcal{L}_2$ discrepancy of order 3 digital nets.

4.1. A bound on the $\mathcal{L}_2$ discrepancy of order 3 digital nets

THEOREM 4.1. *Let $s, m \in \mathbb{N}$. For every (digitally shifted) order 3 digital (t, m, s)-net $\mathcal{P}_{2^m,s}$ over $\mathbb{F}_2$ we have*

$$\mathcal{L}_{2,2^m}(\mathcal{P}_{2^m,s}) \ll_s \frac{m^{(s-1)/2}}{2^{m-t}}.$$

Proof. The proof of Theorem 4.1 can be obtained by specializing the proof of Theorem 1.1 to the case where $r = 1$. In the following we describe the necessary changes in the proof of Theorem 1.1 to obtain the result. The reason for requiring only $\alpha = 3$ instead of $\alpha \ge 5$ is that we do not make use of Lemma 3.6 in this proof.

Let $C_1, \dots, C_s \in \mathbb{F}_2^{3m\times m}$ be the generating matrices of $\mathcal{P}_{2^m s}$ and recall the definition

$$\mathcal{D} = \{\boldsymbol{k} \in \mathbb{N}_0^s : C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s \equiv 0 \pmod 2\}$$

and $\mathcal{D}^* = \mathcal{D} \setminus \{\mathbf{0}\}$. We can use the same argument as in the proof of Theorem 1.1 where $r = 1$. Take $\mathcal{J} = \mathcal{J}_{i,i'}$ and $\mathcal{J}(z) = \mathcal{J}_{i,i'}(z)$ from the proof of

Theorem 1.1 with $i = i'$ and $m_i = m$, i.e., by (14) and (15) we have

$$\mathcal{J} = \{(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{D}^* \times \mathcal{D}^* : r(\boldsymbol{k},\boldsymbol{l}) \neq 0\}.$$
$$\mathcal{J}(z) = \{(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J} : \mu(\boldsymbol{k}) + \mu(\boldsymbol{l}) = z\}.$$

By the same arguments as in the proof of Theorem 1.1 (see (17)), we have

$$\begin{aligned}\mathcal{L}^2_{2,2^m}(\mathcal{P}_{2^m,s}) &= \Big| \sum_{\boldsymbol{k},\boldsymbol{l}\in\mathcal{D}^*} r(\boldsymbol{k},\boldsymbol{l}) \operatorname{wal}_{\boldsymbol{k}}(\boldsymbol{\sigma}) \operatorname{wal}_{\boldsymbol{l}}(\boldsymbol{\sigma})\Big| \\ &\le \sum_{\boldsymbol{k},\boldsymbol{l}\in\mathcal{D}^*} |r(\boldsymbol{k},\boldsymbol{l})| = \sum_{(\boldsymbol{k},\boldsymbol{l})\in\mathcal{J}} |r(\boldsymbol{k},\boldsymbol{l})|\end{aligned}$$

and for $(\boldsymbol{k},\boldsymbol{l}) \in \mathcal{J}$ we have

$$|r(\boldsymbol{k},\boldsymbol{l})| \le \frac{1}{3^s 2^{\mu(\boldsymbol{k})+\mu(\boldsymbol{l})}}.$$

Thus (cf. (18))

$$\mathcal{L}^2_{2,2^m}(\mathcal{P}) \ll_s \sum_{(\boldsymbol{k},\boldsymbol{l})\in\mathcal{J}} \frac{1}{2^{\mu(\boldsymbol{k})+\mu(\boldsymbol{l})}}.$$

It follows from the (order 1) digital (t,m,s)-net property and $\boldsymbol{k} \in \mathcal{D}^*$ that $\mu(\boldsymbol{k}) > m - t$, and from $\boldsymbol{l} \in \mathcal{D}^*$ it also follows that $\mu(\boldsymbol{l}) > m - t$ and hence $\mu(\boldsymbol{k}) + \mu(\boldsymbol{l}) \ge 2(m - t + 1)$. Therefore (cf. Lemma 3.1)

$$\mathcal{L}^2_{2,2^m}(\mathcal{P}) \ll_s \sum_{z=2(m-t+1)}^{\infty} \frac{|\mathcal{J}(z)|}{2^z}. \tag{24}$$

From Lemma 3.7, we find for $z = 2m - 2t + 2 + \kappa$ with $\kappa \ge 0$ that

$$\begin{aligned}&|\mathcal{J}(2m-2t+2+\kappa)| \\ &\quad\le 2^{\kappa/2+2} \sum_{z_1'=0}^{\lceil \kappa/2\rceil} \binom{z_1'+m-t+s}{s-1} \\ &\qquad\times \binom{2(\kappa-z_1')+s+2-t}{s} \binom{3(\kappa-z_1')+s+3-2t}{s}.\end{aligned}$$

Inserting this result into (24) we obtain

$$\begin{aligned}\mathcal{L}^2_{2,2^m}(\mathcal{P}_{2^m,s}) &\ll_s \frac{1}{2^{2m-2t+2}} \sum_{\kappa=0}^{\infty} \frac{|\mathcal{J}(2m-2t+2+\kappa)|}{2^\kappa} \\ &\le \frac{1}{2^{2m-2t}} \sum_{\kappa=0}^{\infty} \frac{1}{2^{\kappa/2}} \sum_{z_1'=0}^{\lceil \kappa/2\rceil} \binom{z_1'+m-t+s}{s-1} \\ &\qquad\times \binom{2(\kappa-z_1')+s+2-t}{s} \binom{3(\kappa-z_1')+s+3-2t}{s}\end{aligned}$$

$$\leq \frac{1}{2^{2m-2t}} \sum_{\kappa=0}^{\infty} \frac{\kappa/2+1}{2^{\kappa/2}} \frac{(\kappa+1+m-t+s)^{s-1}}{(s-1)!} \times \frac{(2\kappa+s+2-t)^s}{s!} \frac{(3\kappa+s+3-2t)^s}{s!}.$$

Since the sum over κ is now from 0 to ∞, we do not need to use Lemma 3.6. Thus also the assumption that $\alpha \geq 5$ is not needed and $\alpha = 3$ is sufficient.

Using the fact that t depends only on the dimension s, we therefore obtain

$$\mathcal{L}^2_{2,2^m}(\mathcal{P}_{2^m,s}) \ll_s \frac{m^{s-1}}{2^{2m-2t}} \sum_{\kappa=0}^{\infty} \frac{\kappa^{3s}}{2^{\kappa/2}} \ll_s \frac{m^{s-1}}{2^{2m-2t}}.$$

Thus the result follows by taking the square root. ∎

4.2. The proof of Corollary 1.3. This proof uses Theorem 4.1 and an idea from [7].

Proof. For an integer $N \geq 2$ we choose $m \in \mathbb{N}$ such that $2^{m-1} < N \leq 2^m$. Let $\mathcal{P}_{2^m,s}$ be an order 3 digital (t,m,s)-net over $\mathbb{F}_2$ with the property that the first component of $\mathcal{P}_{2^m,s}$ is a $(0,m,1)$-net over $\mathbb{F}_2$. Note that such nets exist for every m and can be obtained in the following way: Take the digital sequence introduced in Section 1.2 in dimension $3s-1$. Concatenate to the nth element the component $n2^{-m}$ for $n = 0, 1, \ldots, 2^m - 1$, so that the new points are of the form $(n2^{-m}, y_{n,1}, y_{n,2}, \ldots, y_{n,3s-1})$, where $(y_{n,1}, \ldots, y_{n,3s-1})$ is the nth point of the sequence. Then the set consisting of the points $(n2^{-m}, y_{n,1}, y_{n,2})$ for $0 \leq n < 2^m$ is a digital $(0,m,3)$-net. Apply the digit interlacing composition to the point set

$$\{(n2^{-m}, y_{n,1}, y_{n,2}, \ldots, y_{n,3s-1}) : n = 0, 1, \ldots, 2^m - 1\}.$$

We can now use [13, Proposition 1], which states the following: Let $C_1, \ldots, C_{\alpha s}$ be the generating matrices of a digital (t,m,s)-net and let $C_1^{(\alpha)}, \ldots, C_s^{(\alpha)}$ be the matrices obtained by applying the interlacing construction to $C_1, \ldots, C_{\alpha s}$. Then $C_1^{(\alpha)}, \ldots, C_s^{(\alpha)}$ are generating matrices of an order 3 digital (t,m,s)-net. In particular, it follows that the first component of the order 3 digital net obtained this way is a digital $(0,m,1)$-net.

We now proceed as in [7]. According to Theorem 4.1 we have

$$\mathcal{L}_{2,2^m}(\mathcal{P}_{2^m,s}) \ll_s \frac{m^{(s-1)/2}}{2^m}. \tag{25}$$

As shown above, the first component of $\mathcal{P}_{2^m,s}$ is a digital $(0,m,1)$-net over $\mathbb{F}_2$. Hence the subset

$$\widetilde{\mathcal{P}}_{N,s} := \mathcal{P}_{2^m,s} \cap \left(\left[0, \frac{N}{2^m}\right) \times [0,1)^{s-1} \right)$$

contains exactly N points. We define the point set

$$\mathcal{P}_{N,s} := \left\{ \left(\frac{2^m}{N} x_1, x_2, \ldots, x_s \right) \,:\, (x_1, x_2, \ldots, x_s) \in \widetilde{\mathcal{P}}_{N,s} \right\}.$$

Then we have (with $\boldsymbol{y} = (y_1, \ldots, y_s)$)

$$\begin{aligned}
(N\mathcal{L}_{2,N}(\mathcal{P}_{N,s}))^2 &= \int_{[0,1]^s} |A([\mathbf{0}, \boldsymbol{y}), N, \mathcal{P}_{N,s})) - N\lambda_s([\mathbf{0}, \boldsymbol{y}))|^2 \, d\boldsymbol{y} \\
&= \int_0^1 \cdots \int_0^1 \left| A\Big([0, y_1 N 2^{-m}) \times \prod_{i=2}^{s} [0, y_i), N, \widetilde{\mathcal{P}}_{N,s}\Big) \right. \\
&\qquad \left. - 2^m \frac{N}{2^m} y_1 \ldots y_s \right|^2 dy_1 \cdots dy_s \\
&= \frac{2^m}{N} \int_0^{N/2^m} \int_0^1 \cdots \int_0^1 |A([\mathbf{0}, \boldsymbol{y}), N, \widetilde{\mathcal{P}}_{N,s}) - 2^m \lambda_s([\mathbf{0}, \boldsymbol{y}))|^2 \, d\boldsymbol{y} \\
&= \frac{2^m}{N} \int_0^{N/2^m} \int_0^1 \cdots \int_0^1 |A([\mathbf{0}, \boldsymbol{y}), 2^m, \mathcal{P}_{2^m,s}) - 2^m \lambda_s([\mathbf{0}, \boldsymbol{y}))|^2 \, d\boldsymbol{y} \\
&\le \frac{2^m}{N} (2^m \mathcal{L}_{2,2^m}(\mathcal{P}_{2^m,s}))^2.
\end{aligned}$$

With (25) we get

$$(N\mathcal{L}_{2,N}(\mathcal{P}_{N,s}))^2 \ll_s \frac{2^m}{N} m^{s-1} \ll_s (\log N)^{s-1}.$$

Taking the square root and dividing by N we finally obtain

$$\mathcal{L}_{2,N}(\mathcal{P}_{N,s}) \ll_s \frac{(\log N)^{(s-1)/2}}{N}. \quad \blacksquare$$

Acknowledgments. H. Niederreiter also independently suggested recently that higher order nets may achieve the optimal rate of convergence of the $\mathcal{L}_2$ discrepancy.

J. Dick is supported by a Queen Elizabeth 2 Fellowship of the Australian Research Council. F. Pillichshammer is partially supported by the Austrian Research Foundation (FWF), Project S9609.

References

[1] N. L. Bassily and I. Kátai, *Distribution of the values of q-additive functions on polynomial sequences*, Acta Math. Hungar. 68 (1995), 353–361.

[2] J. Beck and W. W. L. Chen, *Irregularities of Distribution*, Cambridge Univ. Press, Cambridge, 1987.

[3] H. Chaix et H. Faure, *Discrépance et diaphonie en dimension un*, Acta Arith. 63 (1993), 103–141.

[4] W. W. L. Chen, *On irregularities of distribution*, Mathematika 27 (1980), 153–170.
[5] W. W. L. Chen, *On irregularities of distribution II, Quart*, J. Math. Oxford 34 (1983), 257–279.
[6] W. W. L. Chen and M. M. Skriganov, *Davenport's theorem in the theory of irregularities of point distribution*, Zap. Nauch. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 269 (2000), 339–353.
[7] W. W. L. Chen and M. M. Skriganov, *Explicit constructions in the classical mean squares problem in irregularities of point distribution*, J. Reine Angew. Math. 545 (2002), 67–95.
[8] W. W. L. Chen and M. M. Skriganov, *Orthogonality and digit shifts in the classical mean squares problem in irregularities of point distribution*, in: Diophantine Approximation, Dev. Math. 16, Springer, Vienna, 2008, 141–159.
[9] H. E. Chrestenson, *A class of generalized Walsh functions*, Pacific J. Math. 5 (1955), 17–31.
[10] H. Davenport, *Note on irregularities of distribution*, Mathematika 3 (1956), 131–135.
[11] J. Dick, *Explicit constructions of quasi-Monte Carlo rules for the numerical integration of high-dimensional periodic functions*, SIAM J. Numer. Anal. 45 (2007), 2141–2176.
[12] J. Dick, *Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order*, SIAM J. Numer. Anal. 46 (2008), 1519–1553.
[13] J. Dick, *On quasi-Monte Carlo rules achieving higher order convergence*, in: Monte Carlo and Quasi-Monte Carlo Methods 2008, Springer, Berlin, 2009, 73–96. (A preprint is available at roth.cs.kuleuven.be).
[14] J. Dick and F. Pillichshammer, *On the mean square weighted $\mathcal{L}_2$ discrepancy of randomized digital (t, m, s)-nets over $\mathbb{Z}_2$*, Acta Arith. 117 (2005), 371–403.
[15] J. Dick and F. Pillichshammer, *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge Univ. Press, Cambridge, 2010.
[16] J. Dick and F. Pillichshammer, *Explicit constructions of point sets and sequences with low discrepancy*, in: Uniform Distribution and Quasi-Monte Carlo Methods. Discrepancy, Integration and Applications, P. Kritzer et al. (eds.), de Gruyter, Berlin, 2014.
[17] N. M. Dobrovol'skiĭ, *An effective proof of Roth's theorem on quadratic dispersion*, Uspekhi Mat. Nauk 39 (1984), no. 4, 155–156 (in Russian); English transl.: Russian Math. Surveys 39 (1984), no. 4, 117–118.
[18] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, Lecture Notes in Math. 1651, Springer, Berlin, 1997.
[19] H. Faure and F. Pillichshammer, *L_2 discrepancy of two-dimensional digitally shifted Hammersley point sets in base b*, in: Monte Carlo and Quasi-Monte Carlo Methods 2008, P. L'Ecuyer and A. B. Owen (eds.), Springer, Berlin, 2009, 355–368.
[20] H. Faure and F. Pillichshammer, *L_p discrepancy of generalized two-dimensional Hammersley point sets*, Monatsh. Math. 158 (2009), 31–61.
[21] H. Faure, F. Pillichshammer, G. Pirsic and W. Ch. Schmid, *L_2 discrepancy of generalized two-dimensional Hammersley point sets scrambled with arbitrary permutations*, Acta Arith. 141 (2010), 395–418.
[22] N. J. Fine, *On the Walsh functions*, Trans. Amer. Math. Soc. 65 (1949), 372–414.
[23] K. K. Frolov, *Upper bound of the discrepancy in metric L_p, $2 \le p < \infty$*, Dokl. Akad. Nauk SSSR 252 (1980), 805–807 (in Russian); English transl.: Soviet Math. Dokl. 21 (1980), 840–842.
[24] V. S. Grozdanov, *On the diaphony of one class of one-dimensional sequences*, Int. J. Math. Math. Sci. 19 (1996), 115–124.

[25] P. Kritzer and F. Pillichshammer, *An exact formula for the L_2 discrepancy of the shifted Hammersley point set*, Unif. Distrib. Theory 1 (2006), 1–13.

[26] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley, New York, 1974; reprint, Dover, Mineola, NY, 2006.

[27] G. Larcher and F. Pillichshammer, *Walsh series analysis of the $\mathcal{L}_2$-discrepancy of symmetrisized point sets*, Monatsh. Math. 132 (2001), 1–18.

[28] G. Larcher and F. Pillichshammer, *Moments of the weighted sum-of-digits function*, Quaest. Math. 28 (2005), 321–336.

[29] G. Larcher and C. Traunfellner, *On the numerical integration of Walsh series by number-theoretic methods*, Math. Comp. 63 (1994), 277–291.

[30] E. Manstavičius, *Probabilistic theory of additive functions related to systems of numeration*, in: New Trends in Probability and Statistics, Vol. 4 (Palanga, 1996), VSP, Utrecht, 1997, 413–429.

[31] J. Matoušek, *Geometric Discrepancy. An Illustrated Guide*, Algorithms Combin. 18, Springer, Berlin, 1999.

[32] H. Niederreiter, *Application of Diophantine approximations to numerical integration*, in: Diophantine Approximation and Its Applications (Washington, DC, 1972), Academic Press, New York, 1973, 129–199.

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

[34] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Reg. Conf. Ser. Appl. Math. 63, SIAM, Philadelphia, 1992.

[35] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[36] P. D. Proinov, *On the L^2 discrepancy of some infinite sequences*, Serdica 11 (1985), 3–12.

[37] P. D. Proinov, *Symmetrization of the van der Corput generalized sequences*, Proc. Japan Acad. Ser. A Math. Sci. 64 (1988), 159–162.

[38] P. D. Proinov and V. S. Grozdanov, *On the diaphony of the van der Corput–Halton sequence*, J. Number Theory 30 (1988), 94–104.

[39] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), 73–79.

[40] K. F. Roth, *On irregularities of distribution III*, Acta Arith. 35 (1979), 373–384.

[41] K. F. Roth, *On irregularities of distribution IV*, Acta Arith. 37 (1980), 67–75.

[42] M. M. Skriganov, *Lattices in algebraic number fields and uniform distribution mod 1*, Algebra i Analiz 1 (1989), no. 2, 207–228 (in Russian); English transl.: Leningrad Math. J. 1 (1990), 535–558.

[43] M. M. Skriganov, *Constructions of uniform distributions in terms of geometry of numbers*, Algebra i Analiz 6 (1994), no. 3, 200–230 (in Russian); English transl.: St. Petersburg Math. J. 6 (1995), 635–664.

[44] M. M. Skriganov, *Harmonic analysis on totally disconnected groups and irregularities of point distributions*, J. Reine Angew. Math. 600 (2006), 25–49.

[45] M. M. Skriganov, *On the mean values of L_p-discrepancies of point distributions*, Algebra i Analiz 24 (2012), no. 6, 196–225 (in Russian); English transl.: St. Petersburg Math. J. 24 (2013), 991–1012.

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

[47] I. M. Sobol', *On the distribution of points in a cube and the approximate evaluation of integrals*, Zh. Vychisl. Mat. i Mat. Fiz. 7 (1967), 784–802 (in Russian); English transl.: USSR Comput. Meth. Math. Phys. 7 (1967), no. 4, 86–112.

[48] S. Tezuka, *Walsh-spectral test for GFSR pseudorandom numbers*, Comm. ACM 30 (1987), 731–735.

[49] S. Tezuka, *Polynomial arithmetic analogue of Halton sequences*, ACM Trans. Model. Comput. Simul. 3 (1993), 99–107.

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

[51] T. T. Warnock, *Computational investigations of low discrepancy point sets*, in: Applications of Number Theory to Numerical Analysis, Academic Press, New York, 1972, 319–343.

[52] H. Woźniakowski, *Average case complexity of multivariate integration*, Bull. Amer. Math. Soc. (N.S.) 24 (1991), 185–194.

[53] S. K. Zaremba, *Some applications of multidimensional integration by parts*, Ann. Polon. Math. 21 (1968), 85–96.

Josef Dick
School of Mathematics and Statistics
The University of New South Wales
Sydney, NSW 2052, Australia
E-mail: josef.dick@unsw.edu.au

Friedrich Pillichshammer
Institut für Finanzmathematik
Johannes Kepler Universität Linz
Altenbergerstraße 69
A-4040 Linz, Austria
E-mail: friedrich.pillichshammer@jku.at

Received on 6.6.2013 (7475)