ACTA ARITHMETICA
108.2 (2003)

Improved upper bounds for the star discrepancy of digital nets in dimension 3

by

Friedrich Pillichshammer (Linz)

1. Introduction. The concept of digital nets provides at the moment the most efficient method to generate point sets with small star discrepancy D_N^*. The *star discrepancy* of a set of points $\mathbf{x}_0,\dots,\mathbf{x}_{N-1}$ in $[0,1)^d$ is defined by

$$D_N^* = \sup_B \left| \frac{A_N(B)}{N} - \lambda(B) \right|,$$

where the supremum is taken over all subintervals B of $[0,1)^d$ of the form $B=\prod_{i=1}^d [0,b_i)$, $0<b_i\le 1$, $A_N(B)$ denotes the number of i with $\mathbf{x}_i\in B$ and λ is the Lebesgue measure.

A *digital* $(0,s,3)$*-net in base* 2 is a set of $N=2^s$ points $\mathbf{x}_0,\dots,\mathbf{x}_{N-1}$ in $[0,1)^3$ which is generated as follows: Choose three $s\times s$-matrices C_1, C_2 and C_3 over $\mathbb{Z}_2$ with the following property: For all integers $d_1,d_2,d_3\ge 0$ with $d_1+d_2+d_3=s$, the system of the first d_1 rows of C_1 together with the first d_2 rows of C_2 and the first d_3 rows of C_3 is linearly independent over $\mathbb{Z}_2$. Then to construct $\mathbf{x}_n := (x_n^{(1)}, x_n^{(2)}, x_n^{(3)})$ for $0\le n\le 2^s-1$, represent n in base 2:

$$n = n_0 + n_1 2 + \ldots + n_{s-1}2^{s-1}$$

with $n_j\in\{0,1\}$. Now multiply C_i with the vector of digits:

$$C_i(n_0,\dots,n_{s-1})^{\mathrm{T}} =: (y_1^{(i)},\dots,y_s^{(i)})^{\mathrm{T}} \in \mathbb{Z}_2^s$$

and set

$$x_n^{(i)} := \sum_{j=1}^s \frac{y_j^{(i)}}{2^j}.$$

Further let us recall the definition of digital $(0,2)$-sequences in base 2: A *digital* $(0,2)$*-sequence in base* 2 is a sequence $\mathbf{x}_0,\mathbf{x}_1,\dots$ in $[0,1)^2$ which is

2000 *Mathematics Subject Classification*: 11K06, 11K38, 42C10.

Key words and phrases: digital nets, digital sequence, star discrepancy, Walsh series analysis.

generated as follows: Choose two $\mathbb{N} \times \mathbb{N}$-matrices C_1 and C_2 over $\mathbb{Z}_2$ such that for every integer $s \geq 1$ the upper left $s \times s$-matrices $C_1(s)$ and $C_2(s)$ generate a digital $(0, s, 2)$-net in base 2 (a digital $(0, s, 2)$-net in base 2 is defined analogously as a digital $(0, s, 3)$-net in base 2—see Section 3). Then to construct $\mathbf{x}_n := (x_n^{(1)}, x_n^{(2)})$ for $n \geq 0$, represent n in base 2:

$$n = n_0 + n_1 2 + n_2 2^2 + \ldots$$

with $n_j \in \{0, 1\}$. Now multiply C_i with the vector of digits:

$$C_i(n_0, n_1, n_2, \ldots)^{\mathrm{T}} =: (y_1^{(i)}, y_2^{(i)}, \ldots)^{\mathrm{T}}$$

and set

$$x_n^{(i)} := \sum_{j=1}^{\infty} \frac{y_j^{(i)}}{2^j}.$$

It was shown by H. Niederreiter in [6] that for the star discrepancy of any digital $(0, s, 3)$-net in base 2 we have

$$N D_N^* \leq \frac{s^2}{4} + \frac{s}{2} + \frac{9}{4}$$

and hence

$$\limsup_{N \to \infty} \max \frac{N D_N^*}{(\log N)^2} \leq \frac{1}{4(\log 2)^2} = 0.5203\ldots,$$

where the maximum is taken over all digital $(0, s, 3)$-nets in base 2 with $N = 2^s$ elements.

Again in [6] Niederreiter proved that for the star discrepancy of the first N elements of a digital $(0, 2)$-sequence in base 2 we have

$$N D_N^* \leq \frac{1}{8(\log 2)^2} (\log N)^2 + \frac{11}{8 \log 2} \log N + \frac{9}{4}$$

and hence

$$\limsup_{N \to \infty} \max \frac{N D_N^*}{(\log N)^2} \leq \frac{1}{8(\log 2)^2} = 0.26017\ldots,$$

where the maximum is taken over all digital $(0, 2)$-sequences in base 2. From this result he concluded for every integer $s \geq 1$ the existence of a digital $(0, s, 3)$-net in base 2 such that

$$N D_N^* \leq s^2/8 + \mathcal{O}(s),$$

where $N = 2^s$.

In [1] H. Faure constructed a digital $(0, 2)$-sequence in base 2 such that

$$\limsup_{N \to \infty} \frac{N D_N^*}{(\log N)^2} \geq \frac{1}{24(\log 2)^2} = 0.0867\ldots$$

In this paper we study the star discrepancy of digital $(0, s, 3)$-nets in base 2 and of digital $(0, 2)$-sequences in base 2. With the help of Walsh series analysis we improve the general bound for the star discrepancy of digital $(0, s, 3)$-nets in base 2 given by Niederreiter (Theorem 1). Further we give an improved upper bound for the star discrepancy of digital $(0, 2)$-sequences in base 2 (Theorem 3) from which we conclude—in the same way as Niederreiter did in [6]—the existence of digital $(0, s, 3)$-nets in base 2 with an essentially smaller bound for the star discrepancy than the general bound given in Theorem 1 (Theorem 2).

2. The results. We have the following general upper bound for the star discrepancy of digital $(0, s, 3)$-nets in base 2. This bound improves the discrepancy bound given in [6].

THEOREM 1. *For all digital* $(0, s, 3)$*-nets in base* 2 *we have*

$$ND_N^* \le s^2/6 + \mathcal{O}(s),$$

where $N = 2^s$*.*

The proof will be given in Section 4. From Theorem 1 we immediately get the following corollary:

COROLLARY 1. *We have*

$$\limsup_{N\to\infty} \max \frac{ND_N^*}{(\log N)^2} \le \frac{1}{6(\log 2)^2} = 0.34689\ldots,$$

where the maximum is taken over all digital $(0, s, 3)$*-nets in base* 2*.*

Actually we can prove the existence of digital $(0, s, 3)$-nets in base 2 with an essentially smaller constant at the leading term in the discrepancy bound as given in Theorem 1. We have

THEOREM 2. *For every* $s \ge 1$ *there exists a digital* $(0, s, 3)$*-net in base* 2 *such that*

$$ND_N^* \le s^2/12 + \mathcal{O}(s),$$

where $N = 2^s$*.*

The proof of this theorem will be given in Section 5. The digital $(0, s, 3)$-nets in base 2 for which the discrepancy bound in Theorem 2 holds are obtained by setting $\mathbf{x}_n = (n/2^s, \mathbf{y}_n)$, $n = 0, \ldots, 2^s - 1$, where $\mathbf{y}_n$ is the nth element of a digital $(0, 2)$-sequence in base 2. We shall see that the above Theorem 2 is a consequence of the following theorem:

THEOREM 3. *For the star discrepancy* D_N^* *of the first* N *elements of a digital* $(0, 2)$*-sequence in base* 2 *we have*

$$ND_N^* \le \frac{1}{12(\log 2)^2} (\log N)^2 + \frac{89}{36 \log 2} \log N + \frac{33}{6}.$$

The proof of this theorem will be given in Section 5. Combining the result from Theorem 3 with the result of Faure [1] mentioned in Section 1 we obtain

Corollary 2. *We have*

$$\frac{1}{24(\log 2)^2} \le \limsup_{N\to\infty} \max \frac{ND_N^*}{(\log N)^2} \le \frac{1}{12(\log 2)^2},$$

where the maximum is taken over all digital $(0,2)$*-sequences in base* 2*.*

3. Notation and auxiliary results. For $0 \le \alpha,\beta,\gamma \le 1$ we consider the discrepancy function

$$\Delta(\alpha,\beta,\gamma) := A_N([0,\alpha)\times[0,\beta)\times[0,\gamma)) - N\alpha\beta\gamma$$

for digital $(0,s,3)$-nets $\mathbf{x}_0,\ldots,\mathbf{x}_{2^s-1}$ in base 2 (i.e. $N=2^s$).

Since the generating matrices C_1, C_2 and C_3 of a $(0,s,3)$-net must be regular, and since multiplying C_1, C_2 and C_3 by a regular matrix A does not change the point set (only its order) we may always assume that

$$C_1 = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \multicolumn{5}{c}{\dotfill} \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} c^2_{1,1} & c^2_{1,2} & \cdots & c^2_{1,s} \\ c^2_{2,1} & c^2_{2,2} & \cdots & c^2_{2,s} \\ \multicolumn{4}{c}{\dotfill} \\ c^2_{s,1} & c^2_{s,2} & \cdots & c^2_{s,s} \end{pmatrix} =: \begin{pmatrix} \vec{c}^{\,2}_1 \\ \vec{c}^{\,2}_2 \\ \vdots \\ \vdots \\ \vec{c}^{\,2}_s \end{pmatrix},$$

$$C_3 = \begin{pmatrix} c^3_{1,1} & c^3_{1,2} & \cdots & c^3_{1,s} \\ c^3_{2,1} & c^3_{2,2} & \cdots & c^3_{2,s} \\ \multicolumn{4}{c}{\dotfill} \\ c^3_{s,1} & c^3_{s,2} & \cdots & c^3_{s,s} \end{pmatrix} =: \begin{pmatrix} \vec{c}^{\,3}_1 \\ \vec{c}^{\,3}_2 \\ \vdots \\ \vdots \\ \vec{c}^{\,3}_s \end{pmatrix}.$$

Assume that α, β and γ are "s-bit", i.e.

$$\alpha = \frac{\alpha_1}{2} + \ldots + \frac{\alpha_s}{2^s}, \qquad \beta = \frac{\beta_1}{2} + \ldots + \frac{\beta_s}{2^s}, \qquad \gamma = \frac{\gamma_1}{2} + \ldots + \frac{\gamma_s}{2^s},$$

and let α', β' and γ' be arbitrary with

$$\alpha \le \alpha' < \alpha + \frac{1}{2^s}, \qquad \beta \le \beta' < \beta + \frac{1}{2^s}, \qquad \gamma \le \gamma' < \gamma + \frac{1}{2^s}.$$

Then (since all coordinates of the points of a digital net are s-bit) we have

$$\Delta(\alpha',\beta',\gamma') = \Delta(\alpha,\beta,\gamma) - 2^s(\alpha'\beta'\gamma' - \alpha\beta\gamma),$$

and hence for the star-discrepancy D_N^* of the net we have

$$\Big| D_N^* - \frac{1}{N} \max_{\substack{\alpha,\beta,\gamma \\ s\text{-bit}}} |\Delta(\alpha,\beta,\gamma)| \Big| < \frac{3}{N} - \frac{3}{N^2} + \frac{1}{N^3} \tag{1}$$

(note that $N = 2^s$).

We will call

$$\frac{1}{N}\max_{\substack{\alpha,\beta,\gamma \\ s\text{-bit}}}|\Delta(\alpha,\beta,\gamma)| =: D_N^{\mathrm{d}}$$

the *discrete discrepancy* of the net. D_N^{d} differs from D_N^* at most by the almost negligible quantity $3/N$ and seems for nets to be the more natural measure for the irregularities of distribution.

We need some further notation: For any s-bit number $\delta = \delta_1/2 + \ldots + \delta_s/2^s$ we write

$$\vec{\delta} := \begin{pmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \delta_s \end{pmatrix},$$

and for a non-negative integer $k = k_{s-1}2^{s-1} + \ldots + k_1 2 + k_0$ we write

$$\vec{k} := \begin{pmatrix} k_0 \\ k_1 \\ \vdots \\ k_{s-1} \end{pmatrix}.$$

For the proof of Theorem 1 we need two auxiliary results.

LEMMA 1. *Let z be of the form $z = p/2^s$, $p \in \{0,\ldots,2^s-1\}$ (i.e. z is s-bit). Then for the characteristic function $\chi_{[0,z)}$ of the interval $[0,z)$ we have*

$$\chi_{[0,z)}(x) = \sum_{k=0}^{2^s-1} c_k(z)\mathrm{wal}_k(x),$$

where wal_k denotes the kth Walsh function in base 2 (see Remark 1),

$$c_k(z) = \begin{cases} z & \text{if } k = 0, \\ \mathrm{wal}_k(z)\,\dfrac{1}{2^{v(k)}}\,\psi(2^{v(k)}z) & \text{if } k \neq 0, \end{cases}$$

where $\psi(x)$ is periodic with period 1 and

$$\psi(x) = \begin{cases} x & \text{if } 0 \le x < 1/2, \\ x-1 & \text{if } 1/2 \le x < 1, \end{cases}$$

and $v(k) = r$ if $2^r \le k < 2^{r+1}$ (for $k = 0$ define $v(0) := -1$).

REMARK 1. Recall that Walsh functions in base 2 can be defined as follows: For a non-negative integer k with base 2 representation $k = k_m 2^m + \ldots + k_1 2 + k_0$ and a real x with (canonical) base 2 representation $x = x_1/2 + x_2/2^2 + \ldots$ we have

$$\mathrm{wal}_k(x) = (-1)^{x_1k_0 + x_2k_1 + \ldots + x_{m+1}k_m} = (-1)^{(\vec{k}|\vec{x})}.$$

Proof of Lemma 1. This is a simple calculation, to be found for example in [3, Lemma 2]. ■

LEMMA 2. *Let ψ be as in Lemma 1. Then*

$$\psi(2^{l+1}\beta)-\sum_{i=0}^{l}\psi(2^i\beta)=\{\beta\}-\beta_{l+2},$$

where $\{\beta\}=\beta-[\beta]$.

Proof. See [4, Lemma 2]. ■

For the proof of Theorem 3 we need some further notation and auxiliary results:

The concept of shifted digital $(0,s,2)$-nets in base 2 is a slight generalization of the well known concept of digital $(0,s,2)$-nets in base 2. A *shifted digital* $(0,s,2)$-*net in base* 2 is a set of $N=2^s$ points $\mathbf{x}_0,\ldots,\mathbf{x}_{N-1}$ in $[0,1)^2$ which is generated as follows: Choose two $s\times s$-matrices C_1, C_2 over $\mathbb{Z}_2$ with the following property: For every integer k, $0\le k\le s$, the system of the first k rows of C_1 together with the first $s-k$ rows of C_2 is linearly independent over $\mathbb{Z}_2$. Further choose two fixed vectors $\vec{k}_i=(k_1^{(i)},\ldots,k_s^{(i)})^{\mathrm{T}}\in\mathbb{Z}_2^s$, $i=1,2$. Then to construct $\mathbf{x}_n:=(x_n^{(1)},x_n^{(2)})$ for $0\le n\le 2^s-1$, represent n in base 2:

$$n=n_0+n_1 2+\ldots+n_{s-1}2^{s-1}$$

with $n_j\in\{0,1\}$. Now multiply C_i with the vector of digits and add the vector $\vec{k}_i$, i.e.:

$$C_i(n_0,\ldots,n_{s-1})^{\mathrm{T}}+\vec{k}_i=:(y_1^{(i)},\ldots,y_s^{(i)})^{\mathrm{T}}\in\mathbb{Z}_2^s$$

and set

$$x_n^{(i)}:=\sum_{j=1}^{s}\frac{y_j^{(i)}}{2^j}.$$

REMARK 2. In the definition of usual digital $(0,s,2)$-nets in base 2 the vectors $\vec{k}_i$, $i=1,2$, are omitted.

For the star discrepancy of shifted digital $(0,s,2)$-nets in base 2 we have the following result:

LEMMA 3. *For the star discrepancy D_N^* of a shifted digital $(0,s,2)$-net in base 2 we have*

$$ND_N^*\le\frac{s}{3}+\frac{19}{9},$$

where $N=2^s$.

Proof. In [4, Theorem 5] this lemma was proved for digital $(0,s,2)$-nets in base 2. It easily follows from the proof that the assertion is also true for shifted digital nets. ■

Finally we need the following general result which is well known in the theory of uniform distribution modulo one:

LEMMA 4. *Let* $\mathbf{x}_0,\dots,\mathbf{x}_{N-1}$ *be a point set in* $[0,1)^d$ *with star discrepancy* D_N^*. *Let* $\mathbf{x}_n := (x_n^{(1)},\dots,x_n^{(d)})$, $0\le n\le N-1$, *and let* $\varepsilon_n^{(i)}$, $0\le n\le N-1$, $1\le i\le d$, *be non-negative reals with* $\varepsilon_n^{(i)} < 1/a$, *such that* $x_n^{(i)}+\varepsilon_n^{(i)}<1$, *for all* $0\le n\le N-1$, $1\le i\le d$. *Then for the star discrepancy* $\widetilde{D}_N^*$ *of the point set* $\widetilde{\mathbf{x}}_0,\dots,\widetilde{\mathbf{x}}_{N-1}$, *with* $\widetilde{x}_n^{(i)} := x_n^{(i)}+\varepsilon_n^{(i)}$ *for all* $0\le n\le N-1$, $1\le i\le d$, *we have*

$$|D_N^*-\widetilde{D}_N^*|\le d/a.$$

4. Proof of Theorem 1. Due to formula (1) it suffices to show that

$$ND_N^{\mathrm{d}}\le s^2/6+\mathcal{O}(s)$$

for all digital $(0,s,3)$-nets in base 2.

Let $I:=[0,\alpha)\times[0,\beta)\times[0,\gamma)$ with α,β and γ s-bit. Then for $\mathbf{y}=(y^{(1)},y^{(2)},y^{(3)})\in[0,1)^3$ by Lemma 1 we have

$$\begin{aligned}
\chi_I(\mathbf{y})-\lambda(I) &= \sum_{\substack{k,l,m=0\\(k,l,m)\ne(0,0,0)}}^{2^s-1} c_k(\alpha)c_l(\beta)c_m(\gamma)\mathrm{wal}_k(y^{(1)})\mathrm{wal}_l(y^{(2)})\mathrm{wal}_m(y^{(3)})\\
&= \alpha\sum_{\substack{l,m=0\\(l,m)\ne(0,0)}}^{2^s-1} c_l(\beta)c_m(\gamma)\mathrm{wal}_l(y^{(2)})\mathrm{wal}_m(y^{(3)})\\
&\quad+\beta\sum_{\substack{k,m=0\\(k,m)\ne(0,0)}}^{2^s-1} c_k(\alpha)c_m(\gamma)\mathrm{wal}_k(y^{(1)})\mathrm{wal}_m(y^{(3)})\\
&\quad+\gamma\sum_{\substack{k,l=0\\(k,l)\ne(0,0)}}^{2^s-1} c_k(\alpha)c_l(\beta)\mathrm{wal}_k(y^{(1)})\mathrm{wal}_l(y^{(2)})\\
&\quad+\sum_{k,l,m=1}^{2^s-1}\mathrm{wal}_k(\alpha)\mathrm{wal}_l(\beta)\mathrm{wal}_m(\gamma)\,\frac{\psi(2^{\upsilon(k)}\alpha)\psi(2^{\upsilon(l)}\beta)\psi(2^{\upsilon(m)}\gamma)}{2^{\upsilon(k)}2^{\upsilon(l)}2^{\upsilon(m)}}\\
&\quad\times\mathrm{wal}_k(y^{(1)})\mathrm{wal}_l(y^{(2)})\mathrm{wal}_m(y^{(3)}).
\end{aligned}$$

Let now $\mathbf{x}_i$, $i=0,\dots,2^s-1$, with $\mathbf{x}_i:=(x_i^{(1)},x_i^{(2)},x_i^{(3)})$ be a digital $(0,s,3)$-

net in base 2. Then we have

$$\begin{aligned}\Delta(\alpha,\beta,\gamma) = \alpha & \sum_{\substack{l,m=0\\(l,m)\neq(0,0)}}^{2^s-1} c_l(\beta)c_m(\gamma)\sum_{i=0}^{2^s-1}\mathrm{wal}_l(x_i^{(2)})\mathrm{wal}_m(x_i^{(3)})\\
&+\beta\sum_{\substack{k,m=0\\(k,m)\neq(0,0)}}^{2^s-1} c_k(\alpha)c_m(\gamma)\sum_{i=0}^{2^s-1}\mathrm{wal}_k(x_i^{(1)})\mathrm{wal}_m(x_i^{(3)})\\
&+\gamma\sum_{\substack{k,l=0\\(k,l)\neq(0,0)}}^{2^s-1} c_k(\alpha)c_l(\beta)\sum_{i=0}^{2^s-1}\mathrm{wal}_k(x_i^{(1)})\mathrm{wal}_l(x_i^{(2)})\\
&+\sum_{k,l,m=1}^{2^s-1}\mathrm{wal}_k(\alpha)\mathrm{wal}_l(\beta)\mathrm{wal}_m(\gamma)\,\frac{\psi(2^{v(k)}\alpha)\psi(2^{v(l)}\beta)\psi(2^{v(m)}\gamma)}{2^{v(k)}2^{v(l)}2^{v(m)}}\\
&\times\sum_{i=0}^{2^s-1}\mathrm{wal}_k(x_i^{(1)})\mathrm{wal}_l(x_i^{(2)})\mathrm{wal}_m(x_i^{(3)})\\
=:{}& \alpha\Sigma_1+\beta\Sigma_2+\gamma\Sigma_3+\Sigma_4.\end{aligned}$$

From [4, Theorem 5] together with the proof of [4, Theorem 1] it follows that

$$|\Sigma_i| \leq \frac{s}{3}+\frac{19}{9}$$

for $i=1,2,3$, and hence it suffices to show that

$$|\Sigma_4| \leq s^2/6+\mathcal{O}(s)$$

for all digital $(0,s,3)$-nets in base 2.

We now consider $\sum_{i=0}^{2^s-1}\mathrm{wal}_k(x_i^{(1)})\mathrm{wal}_l(x_i^{(2)})\mathrm{wal}_m(x_i^{(3)})$ with $x_i^{(1)} := x_{i,1}^{(1)}/2+\ldots+x_{i,s}^{(1)}/2^s$, $x_i^{(2)} := x_{i,1}^{(2)}/2+\ldots+x_{i,s}^{(2)}/2^s$ and $x_i^{(3)} := x_{i,1}^{(3)}/2+\ldots+x_{i,s}^{(3)}/2^s$. We identify $(x_i^{(1)},x_i^{(2)},x_i^{(3)})$ with

$$(x_{i,1}^{(1)},\ldots,x_{i,s}^{(1)},x_{i,1}^{(2)},\ldots,x_{i,s}^{(2)},x_{i,1}^{(3)},\ldots,x_{i,s}^{(3)})^{\mathrm{T}}\in(\mathbb{Z}_2)^{3s}$$

and we define

$$(x_i^{(1)},x_i^{(2)},x_i^{(3)})\oplus(\widetilde{x}_i^{(1)},\widetilde{x}_i^{(2)},\widetilde{x}_i^{(3)}) := (x_{i,1}^{(1)}+\widetilde{x}_{i,1}^{(1)},\ldots,x_{i,s}^{(3)}+\widetilde{x}_{i,s}^{(3)}).$$

Further $\mathrm{wal}_{k,l,m}(x_i^{(1)},x_i^{(2)},x_i^{(3)}) := \mathrm{wal}_k(x_i^{(1)})\mathrm{wal}_l(x_i^{(2)})\mathrm{wal}_m(x_i^{(3)})$, hence

$$\begin{aligned}&\mathrm{wal}_{k,l,m}((x_i^{(1)},x_i^{(2)},x_i^{(3)})\oplus(\widetilde{x}_i^{(1)},\widetilde{x}_i^{(2)},\widetilde{x}_i^{(3)}))\\
&\qquad=\mathrm{wal}_{k,l,m}(x_i^{(1)},x_i^{(2)},x_i^{(3)})\mathrm{wal}_{k,l,m}(\widetilde{x}_i^{(1)},\widetilde{x}_i^{(2)},\widetilde{x}_i^{(3)}),\end{aligned}$$

i.e. $\mathrm{wal}_{k,l,m}$ is a character on $((\mathbb{Z}_2)^{3s},\oplus)$.

The digital net $\mathbf{x}_0, \dots, \mathbf{x}_{2^s-1}$ is a subgroup of $((\mathbb{Z}_2)^{3s}, \oplus)$, hence

$$\sum_{i=0}^{2^s-1} \mathrm{wal}_k(x_i^{(1)})\mathrm{wal}_l(x_i^{(2)})\mathrm{wal}_m(x_i^{(3)}) = \begin{cases} 2^s & \text{if } \mathrm{wal}_{k,l,m}(x_i^{(1)}, x_i^{(2)}, x_i^{(3)}) = 1 \\ & \text{for all } i = 0, \dots, 2^s - 1, \\ 0 & \text{otherwise.} \end{cases}$$

(For more details see [2] or [5].)

Now we have $\mathrm{wal}_{k,l,m}(x_i^{(1)}, x_i^{(2)}, x_i^{(3)}) = (-1)^{(\vec{k}\,|\vec{x}_i^{(1)}) + (\vec{l}\,|\vec{x}_i^{(2)}) + (\vec{m}\,|\vec{x}_i^{(3)})} = 1$ for all $i = 0, \dots, 2^s - 1$ iff

$$(\vec{k}\,|\vec{x}_i^{(1)}) = (\vec{l}\,|\vec{x}_i^{(2)}) + (\vec{m}\,|\vec{x}_i^{(3)}) \quad \text{for all } i = 0, \dots, 2^s - 1$$

(by the definition of the net); this means

$$(\vec{k}\,|\vec{i}\,) = (\vec{l}\,|C_2\vec{i}\,) + (\vec{m}\,|C_3\vec{i}\,) \quad \text{for all } i = 0, \dots, 2^s - 1,$$

and this is satisfied if and only if

$$\vec{k} = C_2^{\mathrm{T}}\vec{l} + C_3^{\mathrm{T}}\vec{m} =: \vec{k}(l, m).$$

Further

$$\mathrm{wal}_{k(l,m),l,m}(\alpha, \beta, \gamma) = \mathrm{wal}_l(\delta)\mathrm{wal}_m(\varepsilon)$$

with $\vec{\delta} := C_2\vec{\alpha} + \vec{\beta}$ and $\vec{\varepsilon} := C_3\vec{\alpha} + \vec{\gamma}$ (note that $\delta_i = (\vec{c}_i^{\,2}|\vec{\alpha}) + \beta_i$ and $\varepsilon_i = (\vec{c}_i^{\,3}|\vec{\alpha}) + \gamma_i$).

Therefore we have

$$\begin{aligned} \Sigma_4 &= 2^s \sum_{\substack{l,m=1 \\ k(l,m)\neq 0}}^{2^s-1} \mathrm{wal}_l(\delta)\mathrm{wal}_m(\varepsilon)\, \frac{\psi(2^{v(k(l,m))}\alpha)\psi(2^{v(l)}\beta)\psi(2^{v(m)}\gamma)}{2^{v(k(l,m))+v(l)+v(m)}} \\ &= 2^s \sum_{u,v=0}^{s-1} \frac{\psi(2^u\beta)\psi(2^v\gamma)}{2^{u+v}} \\ &\quad \times \underbrace{\sum_{l=2^u}^{2^{u+1}-1} \sum_{m=2^v}^{2^{v+1}-1}}_{k(l,m)\neq 0} \mathrm{wal}_l(\delta)\mathrm{wal}_m(\varepsilon)\, \frac{\psi(2^{v(k(l,m))}\alpha)}{2^{v(k(l,m))}}. \end{aligned}$$

For $2^u \le l \le 2^{u+1} - 1$, $2^v \le m \le 2^{v+1} - 1$ we have

$$\begin{aligned} \mathrm{wal}_l(\delta)\mathrm{wal}_m(\varepsilon) &= (-1)^{l_0\delta_1 + \ldots + l_{u-1}\delta_u + \delta_{u+1}}(-1)^{m_0\varepsilon_1 + \ldots + m_{v-1}\varepsilon_v + \varepsilon_{v+1}} \\ &= (-1)^{l_0\delta_1 + \ldots + l_{u-1}\delta_u + m_0\varepsilon_1 + \ldots + m_{v-1}\varepsilon_v} \\ &\quad \times (-1)^{(\vec{c}_{u+1}^{\,2}|\vec{\alpha}) + (\vec{c}_{v+1}^{\,3}|\vec{\alpha}) + \beta_{u+1} + \gamma_{v+1}}, \end{aligned}$$

by the definition of δ and ε. Hence

$$\Sigma_4 = \sum_{u,v=0}^{s-1} \frac{\|2^u\beta\| \cdot \|2^v\gamma\|}{2^{u+v-s}} (-1)^{(\vec{c}^{\,2}_{u+1}+\vec{c}^{\,3}_{v+1}|\vec{\alpha})}$$
$$\times \underbrace{\sum_{l=2^u}^{2^{u+1}-1} \sum_{m=2^v}^{2^{v+1}-1}}_{k(l,m)\neq 0} (-1)^{l_0\delta_1+\ldots+l_{u-1}\delta_u+m_0\varepsilon_1+\ldots+m_{v-1}\varepsilon_v} \frac{\psi(2^{v(k(l,m))}\alpha)}{2^{v(k(l,m))}}.$$

Here $l := l_0 + l_1 2 + \ldots + l_u 2^u$, $m = m_0 + m_1 2 + \ldots + m_v 2^v$ and $\|\cdot\|$ is the distance to the nearest integer function, i.e. $\|x\| := \min(x-[x], 1-(x-[x]))$. Note that $\psi(2^u\beta)(-1)^{\beta_{u+1}} = \|2^u\beta\|$ and $\psi(2^v\gamma)(-1)^{\gamma_{v+1}} = \|2^v\gamma\|$.

For $0 \le u, v \le s-1$ we have

$$\Sigma_5(u,v) := \underbrace{\sum_{l=2^u}^{2^{u+1}-1} \sum_{m=2^v}^{2^{v+1}-1}}_{k(l,m)\neq 0} (-1)^{l_0\delta_1+\ldots+l_{u-1}\delta_u+m_0\varepsilon_1+\ldots+m_{v-1}\varepsilon_v} \frac{\psi(2^{v(k(l,m))}\alpha)}{2^{v(k(l,m))}}$$
$$= \sum_{w=0}^{s-1} \frac{\psi(2^w\alpha)}{2^w} \underbrace{\sum_{l=2^u}^{2^{u+1}-1} \sum_{m=2^v}^{2^{v+1}-1}}_{v(k(l,m))=w} (-1)^{l_0\delta_1+\ldots+l_{u-1}\delta_u+m_0\varepsilon_1+\ldots+m_{v-1}\varepsilon_v}.$$

For $0 \le u, v, w \le s-1$ define

$$\Sigma_6(u,v,w) := \underbrace{\sum_{l=2^u}^{2^{u+1}-1} \sum_{m=2^v}^{2^{v+1}-1}}_{v(k(l,m))=w} (-1)^{l_0\delta_1+\ldots+l_{u-1}\delta_u+m_0\varepsilon_1+\ldots+m_{v-1}\varepsilon_v}$$
$$= \underbrace{\sum_{l=0}^{2^u-1} \sum_{m=0}^{2^v-1}}_{v(k(l+2^u,m+2^v))=w} \mathrm{wal}_l(\delta)\mathrm{wal}_m(\varepsilon).$$

For $0 \le l \le 2^u-1$ and $0 \le m \le 2^v-1$, the condition $v(k(l+2^u, m+2^v)) = w$ means that there are $k_0, \ldots, k_{w-1} \in \mathbb{Z}_2$ such that

$$\vec{c}^{\,2}_1 l_0 + \ldots + \vec{c}^{\,2}_u l_{u-1} + \vec{c}^{\,2}_{u+1} + \vec{c}^{\,3}_1 m_0 + \ldots + \vec{c}^{\,3}_v m_{v-1} + \vec{c}^{\,3}_{v+1}$$
$$+ \vec{e}_1 k_0 + \ldots + \vec{e}_w k_{w-1} + \vec{e}_{w+1} = \vec{0},$$

where $\vec{e}_i$ is the ith canonical vector in $\mathbb{Z}_2^s$ and $\vec{0}$ is the zero vector in $\mathbb{Z}_2^s$.

Since $\vec{c}^{\,2}_1, \ldots, \vec{c}^{\,2}_{u+1}, \vec{c}^{\,3}_1, \ldots, \vec{c}^{\,3}_{v+1}, \vec{e}_1, \ldots, \vec{e}_{w+1}$ by the $(0,s,3)$-net property are linearly independent as long as $(u+1)+(v+1)+(w+1) \le s$ we must have $u+v+w \ge s-2$.

For $0 \le l \le 2^u - 1$ and $0 \le m \le 2^v - 1$, let

$$\vec{n} := (l_0, \ldots, l_{u-1}, m_0, \ldots, m_{v-1})^{\mathrm{T}} \in \mathbb{Z}_2^{u+v}$$

and define

$$\vec{\zeta} := (\delta_1, \ldots, \delta_u, \varepsilon_1, \ldots, \varepsilon_v)^{\mathrm{T}} \in \mathbb{Z}_2^{u+v}.$$

Further let $\mathcal{C}^{(u,v)}$ be the $s \times (u+v)$-matrix over $\mathbb{Z}_2$ given by

$$\mathcal{C}^{(u,v)} := (\vec{c}_1^{\,2}, \ldots, \vec{c}_u^{\,2}, \vec{c}_1^{\,3}, \ldots, \vec{c}_v^{\,3}),$$

and define

$$\vec{d} = \vec{d}(u,v) := \vec{c}_{u+1}^{\,2} + \vec{c}_{v+1}^{\,3} \in \mathbb{Z}_2^s.$$

Now (with this notation) $v(k(l+2^u, m+2^v)) = w$ means

$$\mathcal{C}^{(u,v)}\vec{n} = \begin{pmatrix} k_0 \\ \vdots \\ k_{w-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \vec{d} \tag{2}$$

for some $k_i \in \mathbb{Z}_2$ (therefore in the following we sometimes write $v(k(n)) = w$).

Now we have to consider three cases:

1. $u+v+w = s-2$. Then the matrix $(\mathcal{C}^{(u,v)}, \vec{e}_1, \ldots, \vec{e}_w)$ has rank $s-2$ and therefore the system (2) has one or no solution.

2. $u+v+w = s-1$. Then the matrix $(\mathcal{C}^{(u,v)}, \vec{e}_1, \ldots, \vec{e}_w)$ has rank $s-1$ and therefore the system (2) has one or no solution.

3. $u+v+w \ge s$. Then the matrix $(\mathcal{C}^{(u,v)}, \vec{e}_1, \ldots, \vec{e}_w)$ has rank s and therefore the system (2) has exactly $2^{u+v+w-s}$ solutions.

In the following we give the solutions of the system (2) in the above three cases and calculate the values of $\Sigma_6(u,v,w)$.

1. $u+v+w = s-2$. Since $\vec{e}_1, \ldots, \vec{e}_{w+1}, \vec{c}_1^{\,2}, \ldots, \vec{c}_{u+1}^{\,2}, \vec{c}_1^{\,3}, \ldots, \vec{c}_{v+1}^{\,3}$ are linearly dependent we can find some $\lambda_1^1, \ldots, \lambda_{w+1}^1, \lambda_1^2, \ldots, \lambda_{u+1}^2, \lambda_1^3, \ldots, \lambda_{v+1}^3 \in \mathbb{Z}_2$ not all zero such that

$$\sum_{i=1}^{w+1} \lambda_i^1 \vec{e}_i + \sum_{i=1}^{u+1} \lambda_i^2 \vec{c}_i^{\,2} + \sum_{i=1}^{v+1} \lambda_i^3 \vec{c}_i^{\,3} = \vec{0}.$$

Assume that $\lambda_{w+1}^1 = 0$. Then $\vec{e}_1, \ldots, \vec{e}_w, \vec{c}_1^{\,2}, \ldots, \vec{c}_{u+1}^{\,2}, \vec{c}_1^{\,3}, \ldots, \vec{c}_{v+1}^{\,3}$ are linearly dependent. But this is a contradiction to the $(0,s,3)$-net property and hence $\lambda_{w+1}^1 = 1$. In the same way one can show that $\lambda_{u+1}^2 = 1$ and $\lambda_{v+1}^3 = 1$ and hence the system (2) has exactly one solution.

Now let $D = D(u,v)$ be the following $(u+v)\times(u+v)$-matrix over $\mathbb{Z}_2$:

$$D := \begin{pmatrix} c^2_{1,s-(u+v)+1} & \dots & c^2_{u,s-(u+v)+1} & c^3_{1,s-(u+v)+1} & \dots & c^3_{v,s-(u+v)+1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c^2_{1,s} & \dots & c^2_{u,s} & c^3_{1,s} & \dots & c^3_{v,s} \end{pmatrix}^{-1}$$

(note that $D = D(u,v)$ exists due to the $(0,s,3)$-net property). We have

$$\Sigma_6(u,v,w) = \sum_{\substack{n=0 \\ v(k(n))=w}}^{2^{u+v}-1} (-1)^{(\vec{n}|\vec{\zeta})} = \sum_{\substack{Dn=0 \\ v(k(Dn))=w}}^{2^{u+v}-1} (-1)^{(D\vec{n}|\vec{\zeta})}.$$

Now $v(k(Dn)) = w$ means that

$$\mathcal{C}^{(u,v)} D\vec{n} = \begin{pmatrix} k_0 \\ \vdots \\ k_{w-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \vec{d}$$

for some $k_i \in \mathbb{Z}_2$. This is equivalent to

$$\begin{pmatrix} & & E & & \\ & & & & \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot \vec{n} = \begin{pmatrix} k_0 \\ \vdots \\ k_{w-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} d_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ d_s \end{pmatrix}$$

with

$$E = \begin{pmatrix} c^2_{1,1} & \dots & c^3_{v,1} \\ \dots & \dots & \dots \\ c^2_{1,s-(u+v)} & \dots & c^3_{v,s-(u+v)} \end{pmatrix} \cdot D,$$

i.e. an $(s-(u+v))\times(u+v)$-matrix. Therefore the unique solution $\vec{n}$ is given by

$$\vec{n} = (d_{s-(u+v)+1}, \dots, d_s)^{\mathrm{T}} \in \mathbb{Z}_2^{u+v}$$

and hence for $u+v+w = s-2$ we have

$$\Sigma_6(u,v,w) = (-1)^{((d_{s-(u+v)+1},\dots,d_s)^{\mathrm{T}}|D^{\mathrm{T}}\vec{\zeta})}.$$

2. $u+v+w = s-1$. Let the $(u+v)\times(u+v)$-matrix $D = D(u,v)$ be as in case 1. We consider two subcases:

(a) $u+v \leq s-2$. Assume that $D\vec{n}$ is a solution of the system (2). Then we find as in case 1 that

$$\vec{n} = (d_{s-(u+v)+1}, \dots, d_s)^{\mathrm{T}} \in \mathbb{Z}_2^{u+v}.$$

Let $\vec{r} \in \mathbb{Z}_2^{u+v}$ be the last row of the $(s-(u+v)) \times (u+v)$-matrix

$$E = \begin{pmatrix} c_{1,1}^2 & \dots & c_{v,1}^3 \\ \dots & \dots & \dots \\ c_{1,s-(u+v)}^2 & \dots & c_{v,s-(u+v)}^3 \end{pmatrix} \cdot D.$$

Then $(\vec{r}|\vec{n}) = 1 + d_{s-(u+v)}$; but that contradicts case 1 from which we have $(\vec{r}|\vec{n}) = d_{s-(u+v)}$. Hence system (2) has no solution in this case.

(b) $u+v = s-1$ (hence $w=0$). From $(u+1)+(v+1) = s+1$ we deduce that $\vec{c}_1^{\,2}, \dots, \vec{c}_{u+1}^{\,2}, \vec{c}_1^{\,3}, \dots, \vec{c}_{v+1}^{\,3}$ are linearly dependent. Hence we can find some $\lambda_1, \dots, \lambda_{u+1}, \mu_1, \dots, \mu_{v+1} \in \mathbb{Z}_2$ not all zero such that

$$\sum_{i=1}^{u+1} \lambda_i \vec{c}_i^{\,2} + \sum_{i=1}^{v+1} \mu_i \vec{c}_i^{\,3} = \vec{0}.$$

Assume $\lambda_{u+1} = 0$. Then $\vec{c}_1^{\,2}, \dots, \vec{c}_u^{\,2}, \vec{c}_1^{\,3}, \dots, \vec{c}_{v+1}^{\,3}$ are linearly dependent, which contradicts the $(0,s,3)$-net property. So $\lambda_{u+1} = 1$ and analogously $\mu_{v+1} = 1$. Hence there exists a vector $\vec{n}_0 \in \mathbb{Z}_2^{u+v}$ such that

$$\mathcal{C}^{(u,v)} \vec{n}_0 = \vec{d}. \tag{3}$$

Now consider the following linear equation system:

$$\begin{pmatrix} c_{1,2}^2 & \dots & c_{u,2}^2 & c_{1,2}^3 & \dots & c_{v,2}^3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c_{1,s}^2 & \dots & c_{u,s}^2 & c_{1,s}^3 & \dots & c_{v,s}^3 \end{pmatrix} \cdot \vec{n} = \begin{pmatrix} d_2 \\ \vdots \\ d_s \end{pmatrix}.$$

This system has a unique solution and this solution is $\vec{n}_0$. From this together with (3) it follows that the system

$$\mathcal{C}^{(u,v)} \vec{n} = \vec{e}_1 + \vec{d}$$

cannot have a solution.

Altogether for $u+v+w = s-1$ we have

$$\Sigma_6(u,v,w) = 0.$$

3. $u+v+w \geq s$. We know that system (2) has exactly $2^{u+v+w-s}$ solutions. Again we consider two subcases.

(a) $u+v \leq s$. Let the $(u+v) \times (u+v)$-matrix $D = D(u,v)$ be like in case 1. Proceeding as in case 1 we find that the solutions of system (2) are given by $D\vec{n}$ where

$$\vec{n} = (n_0, \dots, n_{u+v+w-(s+1)}, d_{w+1}+1, d_{w+2}, \dots, d_s)^{\mathrm{T}} \in \mathbb{Z}_2^s, \tag{4}$$

with arbitrary $n_0,\ldots,n_{u+v+w-(s+1)} \in \mathbb{Z}_2$. From this we get

$$\begin{aligned}\Sigma_6(u,v,w) &= \sum_{\substack{Dn=0\\ v(k(Dn))=w}}^{2^{u+v}-1} (-1)^{(D\vec{n}|\vec{\zeta})} = \sum_{\substack{n_0,\ldots,n_{u+v+w-(s+1)}\in\mathbb{Z}_2\\ \vec{n}\text{ as in (4)}}} (-1)^{(\vec{n}\,|D^{\mathrm{T}}\vec{\zeta})}\\ &= (-1)^{((0,\ldots,0,d_{w+1}+1,d_{w+2},\ldots,d_s)^{\mathrm{T}}\,|D^{\mathrm{T}}\vec{\zeta})} \sum_{n=0}^{2^{u+v+w-s}-1} \mathrm{wal}_n(D^{\mathrm{T}}\zeta)\\ &= 2^{u+v+w-s}(-1)^{((0,\ldots,0,d_{w+1}+1,d_{w+2},\ldots,d_s)^{\mathrm{T}}|D^{\mathrm{T}}\vec{\zeta})}\\ &\qquad \times \begin{cases} 1 & \text{if } (D^{\mathrm{T}}\vec{\zeta}\,|\vec{e}_i)=0 \\ & \text{for all } i=1,\ldots,u+v+w-s,\\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

Let $(D^{\mathrm{T}}\vec{\zeta}\,|\vec{e}_i)=0$ for all $i=1,\ldots,u+v+w-s$. Then

$$\begin{aligned}&(D^{\mathrm{T}}\vec{\zeta}\,|(0,\ldots,0,d_{w+1}+1,d_{w+2},\ldots,d_s)^{\mathrm{T}})\\ &\qquad = (D^{\mathrm{T}}\vec{\zeta}\,|(d_{s-(u+v)+1},\ldots,d_s)^{\mathrm{T}}) + (D^{\mathrm{T}}\vec{\zeta}\,|\vec{e}_{u+v+w-s+1}).\end{aligned}$$

Hence for $u+v+w\ge s$, $u+v\le s$ we have

$$\begin{aligned}\Sigma_6(u,v,w) &= 2^{u+v+w-s}(-1)^{(D^{\mathrm{T}}\vec{\zeta}\,|(d_{s-(u+v)+1},\ldots,d_s)^{\mathrm{T}})}\\ &\qquad \times (-1)^{(D^{\mathrm{T}}\vec{\zeta}\,|\vec{e}_{u+v+w-s+1})}\kappa_1(u,v,w,s)\end{aligned}$$

where

$$\kappa_1(u,v,w,s) = \begin{cases} 1 & \text{if } (D^{\mathrm{T}}\vec{\zeta}\,|\vec{e}_i)=0 \text{ for all } i=1,\ldots,u+v+w-s,\\ 0 & \text{otherwise.}\end{cases}$$

(b) $u+v>s$. Let $F=F(u,v)$ be the following $s\times s$-matrix over $\mathbb{Z}_2$:

$$F = (\vec{c}_1^{\,2},\ldots,\vec{c}_u^{\,2},\vec{c}_1^{\,3},\ldots,\vec{c}_{s-u}^{\,3})^{-1}$$

(note that F exists due to the $(0,s,3)$-net property) and let $G=G(u,v)$ be the following $(u+v)\times(u+v)$-matrix over $\mathbb{Z}_2$:

$$G = \left(\begin{array}{ccc|ccc} & & & 0 & \ldots & 0\\ & F & & \vdots & & \vdots\\ & & & 0 & \ldots & 0\\ \hline 0 & \ldots & 0 & 1 & & 0\\ \vdots & & \vdots & & \ddots & \\ 0 & \ldots & 0 & 0 & & 1\end{array}\right).$$

We have

$$(5)\qquad \Sigma_6(u,v,w) = \sum_{\substack{n=0\\ v(k(n))=w}}^{2^{u+v}-1} (-1)^{(\vec{n}|\vec{\zeta})} = \sum_{\substack{Gn=0\\ v(k(Gn))=w}}^{2^{u+v}-1} (-1)^{(G\vec{n}|\vec{\zeta})}.$$

Now $v(k(Gn)) = w$ means that

$$\mathcal{C}^{(u,v)} G\vec{n} = \begin{pmatrix} k_0 \\ \vdots \\ k_{w-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \vec{d}$$

for some $k_i \in \mathbb{Z}_2$. Since

$$\mathcal{C}^{(u,v)} G = (I, \vec{c}^{\,3}_{s-u+1}, \ldots, \vec{c}^{\,3}_{v})$$

where I is the $s \times s$ unit matrix, we get the following solutions for our equation system:

$$\vec{n} = \begin{pmatrix} \vec{d} \\ \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} k_0 \\ \vdots \\ k_{w-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \sum_{i=1}^{u+v-s} r_i \cdot \begin{pmatrix} \vec{c}^{\,3}_{s-u+i} \\ \\ \vec{e}_i \\ \\ \end{pmatrix}$$

for arbitrary $k_i \in \mathbb{Z}_2$ and arbitrary $r_i \in \mathbb{Z}_2$ and where $\vec{e}_i$ is the ith unit vector in $\mathbb{Z}_2^{u+v-s}$.

Let $H = H(u,v)$ be the $(u+v) \times (u+v)$-matrix over $\mathbb{Z}_2$ given by

$$H = \left(\begin{array}{ccc|ccc} c^3_{s-u+1,1} & \ldots & c^3_{v,1} & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ c^3_{s-u+1,s} & \ldots & c^3_{v,s} & 0 & \ldots & 0 \\ \hline 1 & & 0 & 0 & \ldots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & 0 & \ldots & 0 \end{array}\right).$$

Then we can write $\vec{n}$ as

$$\vec{n} = \vec{e}_{w+1} + \begin{pmatrix} \vec{d} \\ \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} k_0 \\ \vdots \\ k_{w-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + H \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_{u+v-s} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where $\vec{e}_{w+1}$ is the $(w+1)$th unit vector in $\mathbb{Z}_2^{u+v}$. Inserting in (5) yields

$$\begin{aligned}\Sigma_6(u,v,w) &= (-1)^{((d_1,\ldots,d_s,0,\ldots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})}(-1)^{(\vec{e}_{w+1}|G^{\mathrm{T}}\vec{\zeta})} \\ &\quad \times \Big(\sum_{k_0,\ldots,k_{w-1}\in\mathbb{Z}_2} (-1)^{((k_0,\ldots,k_{w-1},0,\ldots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})} \Big) \\ &\quad \times \Big(\sum_{r_1,\ldots,r_{u+v-s}\in\mathbb{Z}_2} (-1)^{(H\cdot(r_1,\ldots,r_{u+v-s},0,\ldots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})} \Big) \\ &= (-1)^{((d_1,\ldots,d_s,0,\ldots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})}(-1)^{(\vec{e}_{w+1}|G^{\mathrm{T}}\vec{\zeta})} \\ &\quad \times \Big(\sum_{k=0}^{2^w-1} \mathrm{wal}_k(G^{\mathrm{T}}\zeta) \Big) \Big(\sum_{r=0}^{2^{u+v-s}-1} \mathrm{wal}_r(H^{\mathrm{T}}G^{\mathrm{T}}\zeta) \Big) \\ &= (-1)^{((d_1,\ldots,d_s,0,\ldots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})}(-1)^{(\vec{e}_{w+1}|G^{\mathrm{T}}\vec{\zeta})} \\ &\quad \times 2^{u+v+w-s}\kappa_2(u,v,w,s)\kappa_3(u,v,s),\end{aligned}$$

where

$$\kappa_2(u,v,w,s) = \begin{cases} 1 & \text{if } (\vec{e}_i|G^{\mathrm{T}}\vec{\zeta}) = 0 \text{ for all } i = 1,\ldots,w, \\ 0 & \text{else,} \end{cases}$$

$$\kappa_3(u,v,s) = \begin{cases} 1 & \text{if } (\vec{e}_i|H^{\mathrm{T}}G^{\mathrm{T}}\vec{\zeta}) = 0 \text{ for all } i = 1,\ldots,u+v-s, \\ 0 & \text{else.} \end{cases}$$

Now we can evaluate $\Sigma_5(u,v)$: We consider three cases.

1. $u+v > s$. Then

$$\begin{aligned}\Sigma_5(u,v) &= 2^{u+v-s}(-1)^{((d_1,\ldots,d_s,0,\ldots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})}\kappa_3(u,v,s) \\ &\quad \times \sum_{w=0}^{s-1} \psi(2^w\alpha)(-1)^{(\vec{e}_{w+1}|G^{\mathrm{T}}\vec{\zeta})}\kappa_2(u,v,w,s).\end{aligned}$$

For $0 \le u,v \le s-1$ let

$$m = m(u,v) := \max\{1 \le j \le u+v : (\vec{e}_i|G^{\mathrm{T}}\vec{\zeta}) = 0,\ i = 1,\ldots,j\}$$

(if $u+v=0$ or if $(\vec{e}_1|G^{\mathrm{T}}\vec{\zeta}) = 1$ set $m = m(u,v) := 0$). By the definition of $m = m(u,v)$ we have $(\vec{e}_1|G^{\mathrm{T}}\vec{\zeta}) = \ldots = (\vec{e}_m|G^{\mathrm{T}}\vec{\zeta}) = 0$ and $(\vec{e}_{m+1}|G^{\mathrm{T}}\vec{\zeta}) = 1$.

Hence $\kappa_2(u,v,w,s)=1$ iff $w\le m(u,v)$. So we have

$$\begin{aligned}\Sigma_5(u,v) &= 2^{u+v-s}(-1)^{((d_1,\dots,d_s,0,\dots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})}\kappa_3(u,v,s)\\ &\quad\times\Big(\sum_{w=0}^{m-1}\psi(2^w\alpha)-\psi(2^m\alpha)\Big)\\ &= 2^{u+v-s}(-1)^{((d_1,\dots,d_s,0,\dots,0)^{\mathrm{T}}|G^{\mathrm{T}}\vec{\zeta})}\kappa_3(u,v,s)(\alpha_{m+1}-\alpha),\end{aligned}$$

where we used Lemma 2. Hence

$$|\Sigma_5(u,v)|\le 2^{u+v-s}.$$

2. $u+v\le s-2$. We have

$$\begin{aligned}\Sigma_5(u,v) &= \sum_{w=s-2-(u+v)}^{s-1}\frac{\psi(2^w\alpha)}{2^w}\,\Sigma_6(u,v,w)\\ &= \frac{\psi(2^{s-2-(u+v)}\alpha)}{2^{s-2-(u+v)}}\,\Sigma_6(u,v,s-2-(u+v))\\ &\quad+\sum_{w=s-(u+v)}^{s-1}\frac{\psi(2^w\alpha)}{2^w}\,\Sigma_6(u,v,w)\\ &= 2^{u+v-s}(-1)^{((d_{s-(u+v)+1},\dots,d_s)^{\mathrm{T}}|D^{\mathrm{T}}\vec{\zeta})}\\ &\quad\times\Big[4\psi(2^{s-2-(u+v)}\alpha)+\sum_{w=s-(u+v)}^{s-1}\psi(2^w\alpha)\\ &\quad\times(-1)^{(\vec{e}_{u+v+w-s+1}|D^{\mathrm{T}}\vec{\zeta})}\kappa_1(u,v,w,s)\Big].\end{aligned}$$

For $0\le u,v\le s-1$ let

$$p=p(u,v):=\max\{1\le j\le u+v:(\vec{e}_i|D^{\mathrm{T}}\vec{\zeta})=0,\ i=1,\dots,j\}$$

(if $u+v=0$ or if $(\vec{e}_1|D^{\mathrm{T}}\vec{\zeta})=1$ set $p=p(u,v):=0$). By the definition of $p=p(u,v)$ we have

$$(\vec{e}_1|G^{\mathrm{T}}\vec{\zeta})=\dots=(\vec{e}_p|G^{\mathrm{T}}\vec{\zeta})=0\quad\text{and}\quad(\vec{e}_{p+1}|G^{\mathrm{T}}\vec{\zeta})=1.$$

Hence $\kappa_1(u,v,w,s)=1$ iff $u+v+w-s\le p(u,v)$. So we have

$$\begin{aligned}\Sigma_5(u,v) &= 2^{u+v-s}(-1)^{((d_{s-(u+v)+1},\dots,d_s)^{\mathrm{T}}|D^{\mathrm{T}}\vec{\zeta})}\\ &\quad\times\Big[4\psi(2^{s-2-(u+v)}\alpha)-\psi(2^{s-(u+v)+p}\alpha)+\sum_{w=s-(u+v)}^{s-(u+v)+p-1}\psi(2^w\alpha)\Big].\end{aligned}$$

Now with Lemma 2 we get

$$\begin{aligned}
&\sum_{w=s-(u+v)}^{s-(u+v)+p-1} \psi(2^w\alpha) - \psi(2^{s-(u+v)+p}\alpha) \\
&\qquad = \sum_{w=0}^{s-(u+v)+p-1} \psi(2^w\alpha) - \psi(2^{s-(u+v)+p}\alpha) - \sum_{w=0}^{s-(u+v)-1} \psi(2^w\alpha) \\
&\qquad = \alpha_{s-(u+v)+p+1} - \alpha_{s-(u+v)+1} - \psi(2^{s-(u+v)}\alpha).
\end{aligned}$$

Moreover we have

$$\begin{aligned}
4\psi(2^{s-(u+v)-2}\alpha) &= 4\left(\frac{\alpha_{s-(u+v)}}{2^2} + \ldots + \frac{\alpha_s}{2^{u+v+2}} - \frac{\alpha_{s-(u+v)-1}}{2}\right) \\
&= \alpha_{s-(u+v)} + \{2^{s-(u+v)}\alpha\} - 2\alpha_{s-(u+v)-1}.
\end{aligned}$$

Hence

$$\begin{aligned}
4\psi(2^{s-2-(u+v)}) - \psi(2^{s-(u+v)+p}\alpha) + \sum_{w=s-(u+v)}^{s-(u+v)+p-1} \psi(2^w\alpha) \\
= \alpha_{s-(u+v)} + \{2^{s-(u+v)}\alpha\} - 2\alpha_{s-(u+v)-1} \\
+ \alpha_{s-(u+v)+p+1} - \alpha_{s-(u+v)+1} - \psi(2^{s-(u+v)}\alpha) \\
= \alpha_{s-(u+v)+p+1} + \alpha_{s-(u+v)} - 2\alpha_{s-(u+v)-1}.
\end{aligned}$$

Therefore we have

$$\begin{aligned}
\Sigma_5(u,v) = 2^{u+v-s}(-1)^{((d_{s-(u+v)+1},\ldots,d_s)^{\mathrm{T}}|D^{\mathrm{T}}\vec{\zeta})} \\
\times [\alpha_{s-(u+v)+p+1} + \alpha_{s-(u+v)} - 2\alpha_{s-(u+v)-1}].
\end{aligned}$$

Hence

$$|\Sigma_5(u,v)| \le 2 \cdot 2^{u+v-s}.$$

3. $s-1 \le u+v \le s$. Then we get, as in case 2,

$$\begin{aligned}
\Sigma_5(u,v) = 2^{u+v-s}(-1)^{((d_{s-(u+v)+1},\ldots,d_s)^{\mathrm{T}}|D^{\mathrm{T}}\vec{\zeta})} \\
\times [\alpha_{s-(u+v)+p+1} - \alpha_{s-(u+v)+1} - \psi(2^{s-(u+v)}\alpha)].
\end{aligned}$$

From

$$\begin{aligned}
\psi(2^{s-(u+v)}\alpha) &= \frac{\alpha_{s-(u+v)+2}}{2^2} + \ldots + \frac{\alpha_s}{2^{u+v}} - \frac{\alpha_{s-(u+v)+1}}{2} \\
&= \frac{1}{2}(\{2^{s-(u+v)+1}\alpha\} - \alpha_{s-(u+v)+1})
\end{aligned}$$

we get

$$|\alpha_{s-(u+v)+p+1} - \alpha_{s-(u+v)+1} - \psi(2^{s-(u+v)}\alpha)| = \left|\alpha_{s-(u+v)+p+1} - \frac{1}{2}(\alpha_{s-(u+v)+1} + \{2^{s-(u+v)+1}\alpha\})\right| \le 1$$

and hence

$$|\Sigma_5(u,v)| \le 2^{u+v-s}.$$

Summing up we have

$$|\Sigma_5(u,v)| \le \begin{cases} 2\cdot 2^{u+v-s} & \text{for } u+v \le s-2, \\ 2^{u+v-s} & \text{for } u+v \ge s-1. \end{cases}$$

Therefore

$$\begin{aligned} |\Sigma_4| &\le \sum_{u,v=0}^{s-1} \frac{\|2^u\beta\|\cdot\|2^v\gamma\|}{2^{u+v-s}} \left|\Sigma_5(u,v)\right| \\ &\le \sum_{u,v=0}^{s-1} \|2^u\beta\|\cdot\|2^v\gamma\| + \sum_{\substack{u,v=0\\u+v\le s-2}}^{s-1} \|2^u\beta\|\cdot\|2^v\gamma\|. \end{aligned}$$

From [4, Theorem 3] we get

$$\sum_{u,v=0}^{s-1} \|2^u\beta\|\cdot\|2^v\gamma\| \le \left(\frac{s}{3} + \frac{1}{9} - (-1)^s\frac{1}{9\cdot 2^s}\right)^2.$$

Further, by [4, Theorem 2], we have

$$\begin{aligned} \sum_{\substack{u,v=0\\u+v\le s-2}}^{s-1} \|2^u\beta\|\cdot\|2^v\gamma\| &= \sum_{u=0}^{s-1} \|2^u\beta\| \sum_{v=0}^{s-u-2} \|2^v\gamma\| \\ &\le \sum_{u=0}^{s-1} \|2^u\beta\| \left(\frac{s-u-1}{3} + \frac{1}{9} - \frac{(-1)^{s-u-1}}{9\cdot 2^{s-u-1}}\right) \end{aligned}$$

and

$$\begin{aligned} \sum_{u=0}^{s-1} \|2^u\beta\| \frac{s-u-1}{3} &\le \frac{1}{6} + \frac{1}{3}\sum_{k=1}^{s-2}\sum_{u=0}^{s-k-1} \|2^u\beta\| \\ &\le \frac{1}{6} + \frac{1}{3}\sum_{k=1}^{s-2}\left(\frac{s-k}{3} + \frac{1}{9} - \frac{(-1)^{s-k}}{9\cdot 2^{s-k}}\right) \\ &= \frac{s^2}{18} - \frac{s}{54} - \frac{4}{162} + \frac{(-1)^s}{162\cdot 2^{s-2}}. \end{aligned}$$

Together we have

$$|\Sigma_4| \le \left(\frac{s}{3}+\frac{1}{9}-(-1)^s\,\frac{1}{9\cdot 2^s}\right)^2+\frac{s^2}{18}-\frac{s}{54}-\frac{4}{162}+\frac{(-1)^s}{162\cdot 2^{s-2}}$$
$$+\frac{2}{9}\left(\frac{s}{3}+\frac{1}{9}-(-1)^s\,\frac{1}{9\cdot 2^s}\right)$$
$$=\frac{s^2}{6}+s\cdot\left(\frac{7}{54}-\frac{2(-1)^s}{27\cdot 2^s}\right)+\frac{1}{81}-\frac{2(-1)^s}{81\cdot 2^s}+\frac{1}{81\cdot 2^{2s}}$$

and the result follows. ■

5. Proof of Theorems 2 and 3

Proof of Theorem 3. We use the technique of Niederreiter introduced in [6, Proof of Lemma 4.1] (or see [7, Proof of Lemma 4.11]) and an idea of G. Larcher.

Let $N = b_0 + b_1 2 + \ldots + b_r 2^r$, with $b_r = 1$ and $b_k \in \{0,1\}$, $0 \le k < r$, be the base 2 representation of N and let the integer p be maximal such that 2^p is a divisor of N.

Let the digital $(0,2)$-sequence in base 2 be generated by the $\mathbb{N}\times\mathbb{N}$-matrices C_1 and C_2. Divide the sequence $\mathbf{x}_0,\ldots,\mathbf{x}_{N-1}$ into subsequences $\omega_{m,b}$ for $b = 0,\ldots,b_m-1$ and $m = 0,\ldots,r$, where $\omega_{m,b}$ is the subsequence $\mathbf{x}_n$ with $\sum_{k=m+1}^{r} b_k 2^k + b2^m \le n < \sum_{k=m+1}^{r} b_k 2^k + (b+1)2^m$. For fixed m divide the matrices C_i, $i = 1,2$, into the following parts:

$$C_i = \left(\begin{array}{c|c} C_i(m) & D_i(m) \\ \hline \multicolumn{2}{c}{E_i(m)} \end{array}\right),$$

where $C_i(m)$ is the upper left $m\times m$-submatrix of C_i. If

$$n = \sum_{k=m+1}^{r} b_k 2^k + b2^m + \sum_{k=0}^{m-1} a_k 2^k,$$

then

$$\vec{n} = (a_0, a_1, \ldots, a_{m-1}, b, b_{m+1}, \ldots, b_r, 0, 0, \ldots)^{\mathrm{T}}$$

and

$$C_i\vec{n} = \begin{pmatrix} C_i(m)\cdot\begin{pmatrix} a_0\\ a_1\\ \vdots\\ \vdots\\ a_{m-2}\\ a_{m-1}\end{pmatrix}\\ 0\\ 0\\ \vdots \end{pmatrix} + \begin{pmatrix} D_i(m)\cdot\begin{pmatrix} b\\ b_{m+1}\\ \vdots\\ b_r\\ 0\\ \vdots\end{pmatrix}\\ 0\\ 0\\ \vdots \end{pmatrix} + \begin{pmatrix} 0\\ 0\\ \vdots\\ \vdots\\ \vdots\\ 0\\ \\ E_i(m)\vec{n}\\ \\ \end{pmatrix}.$$

Hence $\omega_{m,b}$ is a modulo $\mathbb{Z}_2$ shifted digital $(0,m,2)$-net in base 2 generated by $C_1(m)$ and $C_2(m)$, which finally is translated by a vector with positive coordinates less than 2^{-m}. Let $\widetilde{\omega}_{m,b}$ be the shifted digital net without the final translation. Let $D^*_{m,b}$ (resp. $\widetilde{D}^*_{m,b}$) be the star discrepancy of $\omega_{m,b}$ (resp. $\widetilde{\omega}_{m,b}$). Then by Lemma 4 we have

$$|D^*_{m,b} - \widetilde{D}^*_{m,b}| \leq \frac{2}{2^m}.$$

Therefore we get, by Lemma 3,

$$\begin{aligned} ND^*_N &\leq \sum_{m=0}^{r}\sum_{b=0}^{b_m-1} 2^m D^*_{m,b} \leq \sum_{m=0}^{r}\sum_{b=0}^{b_m-1} 2^m\left(\frac{2}{2^m} + \widetilde{D}^*_{m,b}\right)\\ &\leq 2\sum_{m=0}^{r} b_m + \sum_{m=0}^{r} b_m\left(\frac{m}{3}+\frac{19}{9}\right)\\ &= 2\sum_{m=p}^{r} b_m + \sum_{m=p}^{r} b_m\left(\frac{m}{3}+\frac{19}{9}\right), \end{aligned}$$

where p is the maximal integer such that 2^p is a divisor of N.

Now apply the same method to the set consisting of the $\mathbf{x}_n$ with $N \leq n \leq 2^{r+1}-1$. This set consists of $2^{r+1}-N$ points. Let

$$2^{r+1} - N = \sum_{m=0}^{r} c_m 2^m,$$

with $c_m \in \{0,1\}$. Again we can split up this set into a union of subsequences. Let $\omega_{m,c}$ for $c = 0,\dots,c_m-1$ and $m = 0,\dots,r$ be the subsequence $\mathbf{x}_n$ with $2^{r+1} - \sum_{k=m+1}^{r} c_k 2^k - c2^m \leq n < 2^{r+1} - \sum_{k=m+1}^{r} c_k 2^k - c2^m + 2^m$. As above one can see that $\omega_{m,c}$ is a modulo $\mathbb{Z}_2$ shifted digital $(0,m,2)$-net in base 2 generated by $C_1(m)$ and $C_2(m)$, which finally is translated by a vector with positive coordinates less than 2^{-m}. As above, for the star discrepancy of our set we get

$$(2^{r+1}-N)D^*_{2^{r+1}-N} \le 2\sum_{m=0}^{r} c_m + \sum_{m=0}^{r} c_m\left(\frac{m}{3}+\frac{19}{9}\right).$$

The first 2^{r+1} points of the $(0,2)$-sequence build a digital $(0,r+1,2)$-net. Our initial set is the difference between this $(0,r+1,2)$-net and the set of $\mathbf{x}_n$ with $N \le n \le 2^{r+1}-1$. Hence

$$ND^*_N \le 2\sum_{m=0}^{r} c_m + \sum_{m=0}^{r} c_m\left(\frac{m}{3}+\frac{19}{9}\right) + \left(\frac{r+1}{3}+\frac{19}{9}\right).$$

Now

$$2^{r+1} = 2^{r+1}-N+N = \sum_{m=0}^{r}(c_m+b_m)2^m.$$

Hence we have $c_0 = \ldots = c_{p-1} = 0$, $b_p + c_p = 2$ and $b_m + c_m = 1$ for $m = p+1, \ldots, r$. Therefore

$$\begin{aligned} ND^*_N \le{}& 2\Big(2-b_p+\sum_{m=p+1}^{r}(1-b_m)\Big) + (2-b_p)\left(\frac{p}{3}+\frac{19}{9}\right) \\ &+ \sum_{m=p+1}^{r}(1-b_m)\left(\frac{m}{3}+\frac{19}{9}\right) + \left(\frac{r+1}{3}+\frac{19}{9}\right). \end{aligned}$$

Hence

$$\begin{aligned} ND^*_N \le \min\Big\{ & 2\sum_{m=p}^{r} b_m + \sum_{m=p}^{r} b_m\left(\frac{m}{3}+\frac{19}{9}\right), \\ & 2\Big(1+\sum_{m=p}^{r}(1-b_m)\Big) + \left(\frac{p}{3}+\frac{19}{9}\right) \\ & + \sum_{m=p}^{r}(1-b_m)\left(\frac{m}{3}+\frac{19}{9}\right) + \left(\frac{r+1}{3}+\frac{19}{9}\right)\Big\}. \end{aligned}$$

Now, since $\min(A,B) \le (A+B)/2$, the result follows. ∎

Finally we give the proof of Theorem 2, which is an easy consequence of Theorem 3.

Proof of Theorem 2. Let $\mathbf{x}_0, \mathbf{x}_1, \ldots$ be a digital $(0,2)$-sequence in base 2 (such a sequence exists by [6, Corollary 6.19]) and let $s \ge 1$ be an integer. Then the set of

$$\mathbf{y}_n := \left(\frac{n}{2^s}, \mathbf{x}_n\right), \qquad n = 0, \ldots, 2^s-1,$$

is a digital $(0, s, 3)$-net in base 2. For the star discrepancy of this net, by [6, Lemma 8.9] and by Theorem 3 we have

$$ND_N^* \leq \frac{1}{12(\log 2)^2}(\log N)^2 + \mathcal{O}(\log N),$$

where $N = 2^s$, and the result follows. ■

Acknowledgments. The author would like to thank Gerhard Larcher for valuable discussions and suggestions.

References

[1] H. Faure, *Discrepancy lower bound in two dimensions*, in: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Lecture Notes in Statist. 106, Springer, 1995, 198–204.

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

[3] G. Larcher and F. Pillichshammer, *Walsh series analysis of the L_2-discrepancy of symmetrisized point sets*, ibid. 132 (2001), 1–18.

[4] —, —, *Sums of distances to the nearest integer and the discrepancy of digital nets*, Acta Arith. 106 (2003), 379–408.

[5] G. Larcher and G. Pirsic, *Base change problems for generalized Walsh series and multivariate numerical integration*, Pacific J. Math. 189 (1999), 75–105.

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

[7] —, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conf. Ser. in Appl. Math. 63, SIAM, Philadelphia, 1992.

Institut für Analysis
Universität Linz
Altenbergerstraße 69
A-4040 Linz, Austria
E-mail: friedrich.pillichshammer@jku.at

Received on 11.2.2002
and in revised form on 6.11.2002 (4217)