Diophantine Approximation
H. P. Schlickewei et al., Editors

ORTHOGONALITY AND DIGIT SHIFTS IN THE CLASSICAL MEAN SQUARES PROBLEM IN IRREGULARITIES OF POINT DISTRIBUTION

William W. L. Chen[1] and Maxim M. Skriganov[2]
[1] *Department of Mathematics, Macquarie University, Sydney, NSW 2109, Australia*
wchen@maths.mq.edu.au
[2] *Steklov Mathematical Institute, Fontanka 27, St. Petersburg 191011, Russia*
skrig@pdmi.ras.ru

To Wolfgang Schmidt on the occasion of his 70th birthday

1 Introduction

Suppose that $\mathcal{A}_N$ is a distribution of $N > 1$ points, not necessarily distinct, in the n-dimensional unit cube $U^n = [0, 1)^n$, where $n \geq 2$. We consider the L_2-discrepancy

$$\mathcal{L}_2[\mathcal{A}_N] = \left(\int_{U^n} |\mathcal{L}[\mathcal{A}_N; Y]|^2 \, \mathrm{d}Y \right)^{1/2},$$

where for every $Y = (y_1, \ldots, y_n) \in U^n$, the local discrepancy $\mathcal{L}[\mathcal{A}_N; Y]$ is given by

$$\mathcal{L}[\mathcal{A}_N; Y] = \#(\mathcal{A}_N \cap B_Y) - N \operatorname{vol} B_Y.$$

Here

$$B_Y = [0, y_1) \times \ldots \times [0, y_n) \subseteq U^n$$

is a rectangular box of volume $\operatorname{vol} B_Y = y_1 \ldots y_n$, and $\#(\mathcal{S})$ denotes the number of points of a set $\mathcal{S}$, counted with multiplicity.

Roth [12,13] established a lower bound for the L_2-discrepancy in any given dimension $n \geq 2$, as well as a corresponding upper bound. More precisely, for every distribution $\mathcal{A}_N$ of N points in the unit cube U^n, we have

$$\mathcal{L}_2[\mathcal{A}_N] > c_n (\log N)^{(n-1)/2},$$

where the positive constant c_n depends only on the dimension n. Furthermore, there exist distributions $\mathcal{B}_N$ of N points in the unit cube U^n such that

Keywords. Irregularities of distribution, orthogonality, digit shift, coding theory.

2000 Mathematics subject classification. 11K38.

$$\mathcal{L}_2[\mathcal{B}_N] < C_n(\log N)^{(n-1)/2}, \tag{1}$$

where the positive constant C_n again depends only on the dimension n.

However, Roth's upper bound technique involves a probabilistic argument, as are the subsequent arguments of Chen [1,2], Frolov [7], Dobrovol'skiĭ [4] and Skriganov [15,16], and no explicit distribution $\mathcal{B}_N$ is given in any of these papers.

The first explicit constructions of such distributions in any dimension $n \geq 2$ can be found in a recent paper of Chen and Skriganov [3], where it is shown that for every integer $N > 1$, a distribution $\mathcal{D}_N$ of N points in the unit cube U^n can be constructed explicitly to satisfy the inequality

$$\mathcal{L}_2[\mathcal{D}_N] < 2^{n+1} p^{2n} \left(\frac{\log N}{\log p} + 2n + 1 \right)^{(n-1)/2}, \tag{2}$$

where $p \geq 2n^2$ is a prime. An important concept of the approach in [3] is the use of suitably generalized Walsh functions which form an orthonormal basis of the space $L_2(U^n)$. One then shows that under suitable conditions, a collection of functions that arise as coefficients of the Fourier–Walsh series of approximations to the characteristic functions of rectangular boxes B_Y is *quasi-orthonormal*.

In this paper, we shall make use of the fact that under suitable conditions, many relevant subcollections of these functions are in fact orthogonal, as has been observed by Skriganov [18] in his recent work on L_q-discrepancy. This enables us to substantially simplify a major aspect of the proof in [3]. We establish the following improvement of the inequality (2).

Theorem 1. *Let $p \geq 2n^2$ be a prime. Then for every $N > 1$, a distribution $\mathcal{D}_N$ of N points in the unit cube U^n can be constructed explicitly to satisfy the inequality*

$$\mathcal{L}_2[\mathcal{D}_N] < 2^{1-n} p^{2n} \left(\frac{\log N}{\log p} + 2n + 1 \right)^{(n-1)/2}. \tag{3}$$

Note that the constant in the inequality (3) is not best possible, but it represents a savings of a factor 4^n from that in the inequality (2) nevertheless. We remark that it is not the main purpose of our work here to improve such constants.

Upper bounds of the form (1) have been given in Roth [13] or in Chen [2] with the constants C_n given implicitly or inductively. In particular, this is achieved in [2] by the use of digit shifts. Here we shall show that digit shifts are in fact intimately related to the orthogonality property mentioned above. We establish the following existence result with explicitly given values for C_n, again not sharp.

Theorem 2. *Let $p \geq n - 1$ be a prime. Then for every $N > 1$, there exists a distribution $\mathcal{D}_N$ of N points in the unit cube U^n which satisfies the inequality*

$$\mathcal{L}_2[\mathcal{D}_N] < 2^{1-n} p^{n+1/2} \left(\frac{\log N}{\log p} + 2 \right)^{(n-1)/2}. \tag{4}$$

Throughout, the letter p denotes a prime number. We shall be concerned with point sets that possess the structure of vector spaces over the finite field

$$\mathbf{F}_p = \{0, 1, \ldots, p-1\}$$

of residues modulo p. We shall discuss these point sets in Section 2, together with an inner product and two special metrics central to our argument. In particular, we shall state a number of results concerning these point sets, which we shall combine in Section 3 with crucial results from our work in [3] to establish Theorem 1. We then deduce Theorem 2 in Section 4, where we need a crucial result of Faure [5].

The remainder of the paper is devoted to the establishment of all the results stated in Section 2, and is organized as follows. In Section 5, we recall necessary facts on generalized Walsh functions. In Section 6, we extend the two special metrics introduced in Section 2 to n-tuples of nonnegative integers in order to cement the intimate relationship between our point sets and the generalized Walsh functions. In Section 7, we consider a suitable approximation of the discrepancy function which can be described by a suitably truncated Fourier–Walsh series. By making use of the roles played by orthogonality and digit shifts, we establish an expression for certain mean squares of this approximation in terms of integrals over Fourier–Walsh coefficients. Finally, we deduce Theorem 5 in Section 8 and Theorems 3 and 4 in Section 9.

For convenience, $\mathbf{N}$ denotes the set of all positive integers, $\mathbf{N}_0$ denotes the set of all nonnegative integers, $\mathbf{Z}$ denotes the set of all integers, $\mathbf{Q}$ denotes the set of all rational numbers, and $\mathbf{C}$ denotes the set of all complex numbers. If $z \in \mathbf{C}$, then $\overline{z} \in \mathbf{C}$ denotes its complex conjugate. Finally, if $\mathcal{S}$ is a finite set, then $\#(\mathcal{S})$ denotes the number of elements of $\mathcal{S}$.

2 Linear distributions

We shall be concerned with a class of sets $D \subset U^n$ which possess the structure of vector spaces over the finite field $\mathbf{F}_p$. For any $s \in \mathbf{N}_0$, let

$$\mathbf{Q}(p^s) = \{mp^{-s} : m = 0, 1, \ldots, p^s - 1\}.$$

Observe that any $x \in \mathbf{Q}(p^s)$ can be represented uniquely in the form

$$x = \sum_{i=1}^{s} \eta_i(x) p^{-i},$$

where the coefficients $\eta_i(x) \in \mathbf{F}_p$ for every $i = 1, \ldots, s$.

For any two vectors $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ in $\mathbf{Q}^n(p^s)$ and any two scalars $\alpha, \beta \in \mathbf{F}_p$, we write

$$\alpha X \oplus \beta Y = (\alpha x_1 \oplus \beta y_1, \ldots, \alpha x_n \oplus \beta y_n) \in \mathbf{Q}^n(p^s) \tag{5}$$

by setting

$$\eta_i(\alpha x_j \oplus \beta y_j) = \alpha \eta_i(x_j) + \beta \eta_i(y_j) \pmod{p}$$

for every $i = 1, \ldots, s$ and $j = 1, \ldots, n$. It is easy to see that with respect to the arithmetic operations (5), the set $\mathbf{Q}^n(p^s)$ forms a vector space of dimension ns over the finite field $\mathbf{F}_p$.

We say that a subset $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution (in base p) if D is a subspace of the vector space $\mathbf{Q}^n(p^s)$.

Suppose now that $s \in \mathbf{N}_0$ is chosen and fixed. Then any $x \in \mathbf{Q}(p^s)$ can also be represented in the form

$$x = \sum_{i=1}^{s} \xi_i(x) p^{i-s-1}, \tag{6}$$

where $\xi_i(x) = \eta_{s+1-i}(x) \in \mathbf{F}_p$ for every $i = 1, \ldots, s$. Using this representation, we can define an inner product on the space $\mathbf{Q}^n(p^s)$ as follows. For every $x, y \in \mathbf{Q}(p^s)$, we let

$$\langle x, y \rangle = \langle y, x \rangle = \sum_{i=1}^{s} \xi_i(x) \xi_{s+1-i}(y).$$

For vectors $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ in $\mathbf{Q}^n(p^s)$, we write

$$\langle X, Y \rangle = \langle Y, X \rangle = \sum_{j=1}^{n} \langle x_j, y_j \rangle.$$

For any linear distribution $D \subseteq \mathbf{Q}^n(p^s)$, where $s \in \mathbf{N}_0$, we now define the dual distribution $D^\perp \subseteq \mathbf{Q}^n(p^s)$ by

$$D^\perp = \{X \in \mathbf{Q}^n(p^s) : \langle X, Y \rangle = 0 \text{ for every } Y \in D\}.$$

It is easy to check that $D^\perp$ is a subspace of $\mathbf{Q}^n(p^s)$, and is therefore also a linear distribution. Furthermore, we have $(D^\perp)^\perp = D$, so that D and $D^\perp$ are mutually dual subspaces of $\mathbf{Q}^n(p^s)$.

Following [3] and [17], we next introduce two metrics on the vector space $\mathbf{Q}^n(p^s)$. For any $x \in \mathbf{Q}(p^s)$, the Hamming weight $\kappa(x)$ is the number of nonzero coefficients $\xi_i(x)$ in the representation (6), while the Rosenbloom–Tsfasman weight is defined by

$$\rho(x) = \begin{cases} 0 & \text{if } x = 0, \\ \max\{i = 1, \ldots, s : \xi_i(x) \neq 0\} & \text{if } x \neq 0; \end{cases}$$

see [11]. For $X = (x_1, \ldots, x_n) \in \mathbf{Q}^n(p^s)$, we now let

$$\kappa(X) = \sum_{j=1}^{n} \kappa(x_j) \quad \text{and} \quad \rho(X) = \sum_{j=1}^{n} \rho(x_j).$$

It is easy to check that $\kappa(X) = \rho(X) = 0$ if and only if $X = 0$. One can also easily check the triangle inequalities for both weights. These give rise to metrics (or distances) on the vector space $\mathbf{Q}^n(p^s)$.

If a linear distribution $D \subseteq \mathbf{Q}^n(p^s)$ contains at least two points, then we can consider the Hamming weight

$$\kappa(D) = \min\{\kappa(X) : X \in D \setminus \{0\}\},$$

and the Rosenbloom–Tsfasman weight

$$\rho(D) = \min\{\rho(X) : X \in D \setminus \{0\}\}.$$

We shall establish the following improvements of Lemma 2D of [3].

Theorem 3. *Suppose that $p \geq 2n^2$ is a prime, and that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ that satisfies $\kappa(D^\perp) \geq 2n+1$ and $\rho(D^\perp) \geq s+1$. Then*

$$\mathcal{L}_2[D] < 2^{1-n} p^n (s+1)^{(n-1)/2}. \tag{7}$$

Theorem 4. *Suppose that $p \geq 2n^2$ is a prime, and that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ that satisfies $\kappa(D^\perp) \geq 2n+1$ and $\rho(D^\perp) \geq s+1$. Then there exists an approximation $\mathcal{M}[D; Y]$ of the discrepancy function $\mathcal{L}[D; Y]$, with error*

$$|\mathcal{L}[D; Y] - \mathcal{M}[D; Y]| \leq n \quad \text{for every } Y \in U^n, \tag{8}$$

such that the quantity

$$\mathcal{M}_2[D] = \left(\int_{U^n} |\mathcal{M}[D; Y]|^2 \, dY \right)^{1/2} \tag{9}$$

can be evaluated precisely. Furthermore, we have

$$\left| (\mathcal{L}_2[D])^2 - (\mathcal{M}_2[D])^2 \right| \leq 2n\mathcal{M}_2[D] + 3n^2. \tag{10}$$

The approximation $\mathcal{M}[D; Y]$ will be given explicitly in Section 7.

For any linear distribution $D \subseteq \mathbf{Q}^n(p^s)$, we can consider cosets of the form

$$D \oplus T = \{X \oplus T : X \in D\}, \tag{11}$$

obtained by applying the same digit shift $T \in \mathbf{Q}^n(p^s)$ to every point of D.

Theorem 5. *Suppose that $p \geq n-1$ is a prime, and that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ that satisfies $\rho(D^\perp) \geq s+1$. Then there exists a digit shift $T \in \mathbf{Q}^n(p^s)$ such that*

$$\mathcal{L}_2[D \oplus T] < 2^{1-n} p^n (s+1)^{(n-1)/2}. \tag{12}$$

The restrictions imposed on the prime p in terms of the dimension n in all our results here can be relaxed if we work with linear distributions with *deficiencies*. More precisely, for each prime p, including $p = 2$, we can explicitly construct linear distributions $D \subset \mathbf{Q}^n(p^s)$ of p^s points with corresponding dual linear distributions $D^\perp \subset \mathbf{Q}^n(p^s)$ satisfying $\rho(D^\perp) \geq s+1-\delta$, where the deficiency δ is a nonnegative integer which depends only on the dimension n and satisfies the bound $\delta = O(n \log n)$. This approach will lead only to a renormalization of the constants in our bounds (7) and (12), but will not necessarily improve the estimates, and so appears to be not worth persuing. However, the benefit of this approach is that with the choice $p = 2$, it is possible to obtain very precise information on the discrepancy of linear distributions in terms of the distribution of the Rosenbloom–Tsfasman weight within the dual linear distributions; see the paragraph after the proof of Lemma 7.5. This leads in turn to very accurate estimates for the mean squares discrepancy of such linear distributions.

3 Deduction of Theorem 1

We shall proceed along the lines of [3], but shall omit some of the details by summarizing lengthy steps as lemmas and giving references where appropriate. Let $g = 2n$, and let $p \geq gn = 2n^2$ be a prime. Given any natural number $N > 1$, we choose $\sigma \in \mathbf{N}$ such that

$$p^{g(\sigma-1)} < N \leq p^{g\sigma}, \tag{13}$$

and consider first of all a linear distribution of $p^{g\sigma}$ points in U^n.

The following result is essentially Lemma 2E of [3].

Lemma 3.1. *Suppose that $p \geq gn$ is a prime, where $g = 2n$. Then for every $\sigma \in \mathbf{N}$, a linear distribution $D(g,\sigma) \subset \mathbf{Q}^n(p^{g\sigma})$ of $p^{g\sigma}$ points can be constructed explicitly, with dual linear distribution $(D(g,\sigma))^\perp \subset \mathbf{Q}^n(p^{g\sigma})$ satisfying*

$$\kappa((D(g,\sigma))^\perp) \geq g+1 \quad \text{and} \quad \rho((D(g,\sigma))^\perp) \geq g\sigma + 1.$$

Clearly the hypotheses of Theorem 3 are satisfied with $g = 2n$ and $s = g\sigma$, and so it follows immediately that

$$\mathcal{L}_2[D(g,\sigma)] < 2^{1-n} p^n (g\sigma+1)^{(n-1)/2}.$$

Our next task is to select a subset of $D(g,\sigma)$ and rescale. Consider the subset

$$\mathcal{D}_N^*(g) = D(g,\sigma) \cap ([0, Np^{-g\sigma}) \times U^{n-1}) \subseteq D(g,\sigma).$$

To guarantee that $\mathcal{D}_N^*(g)$ contains exactly N points, we need the following special case of Lemma 2C of [3] or Theorem 4.2 of [17]. It relates the uniform distribution of the points of a linear distribution D and the spacing of the points of the dual linear distribution $D^\perp$ with respect to the Rosenbloom–Tsfasman metric ρ.

Lemma 3.2. *Suppose that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$. Then the following statements are equivalent:*

(i) *The Rosenbloom–Tsfasman weight $\rho(D^\perp) \geq s+1$.*

(ii) *Every rectangular box of the type*

$$\prod_{j=1}^{n} [m_j p^{-s_j}, (m_j+1)p^{-s_j}) \subset U^n,$$

where $m_1, \ldots, m_n, s_1, \ldots, s_n \in \mathbf{N}_0$ satisfy $s_1 + \ldots + s_n = s$, contains precisely one point of the linear distribution D.

To see that $\mathcal{D}_N^*(g)$ contains exactly N points, we observe simply that every rectangular box of the form $[mp^{-g\sigma}, (m+1)p^{-g\sigma}) \times U^{n-1} \subset U^n$, where $m \in \mathbf{N}_0$, contains exactly one point of $D(g,\sigma)$.

We next rescale $\mathcal{D}_N^*(g)$ to obtain

$$\mathcal{D}_N = \mathcal{D}_N(g) = \{(N^{-1}p^{g\sigma}x_1, x_2, \ldots, x_n) : (x_1, x_2, \ldots, x_n) \in \mathcal{D}_N^*(g)\}.$$

Then in view of (13) and noting that $g = 2n$, we have

$$\int_{U^n} |\mathcal{L}[\mathcal{D}_N; Y]|^2 \, \mathrm{d}Y = N^{-1} p^{g\sigma} \int_{[0, Np^{-g\sigma}) \times U^{n-1}} |\mathcal{L}[D(g, \sigma); Y]|^2 \, \mathrm{d}Y$$

$$\leq N^{-1} p^{g\sigma} \int_{U^n} |\mathcal{L}[D(g, \sigma); Y]|^2 \, \mathrm{d}Y < 4^{1-n} N^{-1} p^{g\sigma} p^{2n} (g\sigma + 1)^{n-1}$$

$$< 4^{1-n} p^g p^{2n} \left(\frac{\log N}{\log p} + g + 1 \right)^{n-1} = 4^{1-n} p^{4n} \left(\frac{\log N}{\log p} + 2n + 1 \right)^{n-1}.$$

The inequality (3) now follows on taking square roots.

4 Deduction of Theorem 2

Let $p \geq n - 1$ be a prime. Given any natural number $N > 1$, we choose $s \in \mathbf{N}$ such that

$$p^{s-1} < N \leq p^s, \tag{14}$$

and consider first of all a linear distribution of p^s points in U^n.

The following result is due to Faure [5]. We remark that the condition $p \geq n - 1$ cannot be relaxed, as observed by Chen [2].

Lemma 4.1. *Suppose that $p \geq n - 1$ is a prime. Then for every $s \in \mathbf{N}$, a linear distribution $D \subset \mathbf{Q}^n(p^s)$ of p^s points can be constructed explicitly such that condition (ii) of Lemma 3.2 is satisfied, so that the dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ has Rosenbloom–Tsfasman weight $\rho(D^\perp) \geq s + 1$.*

It follows from Theorem 5 that there exists a digit shift $T \in \mathbf{Q}^n(p^s)$ such that the inequality (12) holds. Next, observe that condition (ii) of Lemma 3.2 remains valid if we replace the linear distribution D by its coset $D \oplus T$, and so the subset

$$\mathcal{D}_N^* = (D \oplus T) \cap ([0, Np^{-s}) \times U^{n-1}) \subseteq D \oplus T$$

contains exactly N points. We now rescale $\mathcal{D}_N^*$ to obtain

$$\mathcal{D}_N = \{(N^{-1} p^s x_1, x_2, \ldots, x_n) : (x_1, x_2, \ldots, x_n) \in \mathcal{D}_N^*\}.$$

Then in view of (14), we have

$$\int_{U^n} |\mathcal{L}[\mathcal{D}_N; Y]|^2 \, \mathrm{d}Y = N^{-1} p^s \int_{[0, Np^{-s}) \times U^{n-1}} |\mathcal{L}[D \oplus T; Y]|^2 \, \mathrm{d}Y$$

$$\leq N^{-1} p^s \int_{U^n} |\mathcal{L}[D \oplus T; Y]|^2 \, \mathrm{d}Y < 4^{1-n} N^{-1} p^s p^{2n} (s + 1)^{n-1}$$

$$< 4^{1-n} p^{2n+1} \left(\frac{\log N}{\log p} + 2 \right)^{n-1}.$$

The inequality (4) now follows on taking square roots.

5 Walsh functions

Every $\ell \in \mathbf{N}_0$ can be written uniquely in the form

$$\ell = \sum_{i=1}^{\infty} \lambda_i(\ell) p^{i-1}, \tag{15}$$

where the coefficients $\lambda_i(\ell) \in \mathbf{F}_p$ for every $i \in \mathbf{N}$.

For any two vectors $L = (\ell_1, \ldots, \ell_n)$ and $K = (k_1, \ldots, k_n)$ in $\mathbf{N}_0^n$ and any two scalars $\alpha, \beta \in \mathbf{F}_p$, we write

$$\alpha L \oplus \beta K = (\alpha\ell_1 \oplus \beta k_1, \ldots, \alpha\ell_n \oplus \beta k_n) \in \mathbf{N}_0^n \tag{16}$$

by setting

$$\lambda_i(\alpha\ell_j \oplus \beta k_j) = \alpha\lambda_i(\ell_j) + \beta\lambda_i(k_j) \pmod{p}$$

for every $i \in \mathbf{N}$ and $j = 1, \ldots, n$. It is easy to see that with respect to the arithmetic operations (16), the set $\mathbf{N}_0^n$ forms a vector space over the finite field $\mathbf{F}_p$.

On the other hand, every $x \in U$ can be represented in the form

$$x = \sum_{i=1}^{\infty} \eta_i(x) p^{-i}, \tag{17}$$

where the coefficients $\eta_i(x) \in \mathbf{F}_p$ for every $i \in \mathbf{N}$, and this representation is unique if we agree that the series in (17) is finite if

$$x \in \mathbf{Q}(p^\infty) = \bigcup_{s=0}^{\infty} \mathbf{Q}(p^s).$$

In this case, for any two vectors $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ in $\mathbf{Q}^n(p^\infty)$ and any two scalars $\alpha, \beta \in \mathbf{F}_p$, we can extend (5) to

$$\alpha X \oplus \beta Y = (\alpha x_1 \oplus \beta y_1, \ldots, \alpha x_n \oplus \beta y_n) \in \mathbf{Q}^n(p^\infty) \tag{18}$$

by setting

$$\eta_i(\alpha x_j \oplus \beta y_j) = \alpha\eta_i(x_j) + \beta\eta_i(y_j) \pmod{p}$$

for every $i \in \mathbf{N}$ and $j = 1, \ldots, n$. It is easy to see that with respect to the arithmetic operations (18), the set $\mathbf{Q}^n(p^\infty)$ forms a vector space over the finite field $\mathbf{F}_p$.

For every $\ell \in \mathbf{N}_0$ and every $x \in U$, we let

$$w_\ell(x) = e_p\left(\sum_{i=1}^{\infty} \lambda_i(\ell)\eta_i(x)\right), \tag{19}$$

where $e_p(z) = \mathrm{e}^{2\pi \mathrm{i} z/p}$ for every real number z, and where the coefficients $\lambda_i(\ell)$ and $\eta_i(x)$ are given by (15) and (17) respectively. The functions w_ℓ are known as the Walsh functions if $p = 2$ and the Chrestenson or Chrestenson–Levy functions if $p > 2$. For simplicity, we refer to them all as Walsh functions here. A detailed study of such

functions can be found in [8] or [14]. Here it suffices to mention that while $w_0(x) = 1$ for every $x \in U$, we have

$$\int_U w_\ell(x)\,dx = 0 \quad \text{for every } \ell \in \mathbf{N}. \tag{20}$$

For every $L = (\ell_1, \ldots, \ell_n) \in \mathbf{N}_0^n$ and every $X = (x_1, \ldots, x_n) \in U^n$, we let

$$W_L(X) = \prod_{j=1}^{n} w_{\ell_j}(x_j). \tag{21}$$

It is well known that

$$W_{L\oplus K}(X) = W_L(X)W_K(X) \quad \text{for every } X \in U^n \text{ and } L, K \in \mathbf{N}_0^n, \tag{22}$$

and that

$$W_L(X \oplus Y) = W_L(X)W_L(Y) \quad \text{for every } X, Y \in \mathbf{Q}^n(p^\infty) \text{ and } L \in \mathbf{N}_0^n. \tag{23}$$

Furthermore, for every $K, L \in \mathbf{N}_0^n$, we have

$$\int_{U^n} W_K(X)\overline{W_L(X)}\,dX = \int_{U^n} W_{K\ominus L}(X)\,dX = \begin{cases} 1 & \text{if } K = L, \\ 0 & \text{if } K \neq L. \end{cases}$$

Indeed, the Walsh functions form an orthonormal basis of the Hilbert space $L_2(U^n)$ of square-integrable functions on the n-dimensional unit cube U^n. For each $f \in L_2(U^n)$, we have the Fourier–Walsh expansion

$$f(X) \simeq \sum_{L\in\mathbf{N}_0^n} \widetilde{f}_L \overline{W_L(X)},$$

where the symbol $\simeq$ denotes that the series converges in the L_2-norm, and where the Fourier–Walsh coefficients are given by

$$\widetilde{f}_L = \int_{U^n} W_L(X) f(X)\,dX.$$

Known results on characters of abelian groups (cf. [9]) can often be restated in terms of Walsh functions. Here we need the following result. Let

$$\mathbf{N}_0^n(p^s) = \{L = (\ell_1, \ldots, \ell_n) \in \mathbf{N}_0^n : 0 \le \ell_j < p^s \text{ for every } j = 1, \ldots, n\}.$$

The mapping

$$\theta : \mathbf{Q}^n(p^s) \to \mathbf{N}_0^n(p^s) : (x_1, \ldots, x_n) \mapsto (p^s x_1, \ldots, p^s x_n) \tag{24}$$

is clearly an isomorphism of vector spaces.

Lemma 5.1. *For every linear distribution $D \subseteq \mathbf{Q}^n(p^s)$ and every $L \in \mathbf{N}_0^n(p^s)$, we have*

$$\sum_{X\in D} W_L(X) = \begin{cases} \#(D) & \text{if } L \in \theta(D^\perp), \\ 0 & \text{if } L \notin \theta(D^\perp), \end{cases}$$

where $\theta(D^\perp) = \{\theta(Y) : Y \in D^\perp\}$ *denotes the image under the mapping* (24) *of the dual linear distribution* $D^\perp \subseteq \mathbf{Q}^n(p^s)$.

A special case of this is the useful orthogonality result below.

Lemma 5.2. *For every* $L', L'' \in \mathbf{N}_0^n(p^s)$, *we have*

$$\sum_{T \in \mathbf{Q}^n(p^s)} \overline{W_{L'}(T)}\, W_{L''}(T) = \begin{cases} p^{ns} & \text{if } L' = L'', \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

6 More weights and metrics

In Section 2, we considered Hamming and Rosenbloom–Tsfasman weights defined on elements in $\mathbf{Q}^n(p^s)$. The purpose of this section is to consider their analogues on $\mathbf{N}_0^n$.

For any $\ell \in \mathbf{N}_0$, the Hamming weight $\kappa(\ell)$ denotes the number of non-zero coefficients $\lambda_i(\ell)$ in the representation (15), while the Rosenbloom–Tsfasman weight is defined by

$$\rho(\ell) = \begin{cases} 0 & \text{if } \ell = 0, \\ \max\{i \in \mathbf{N} : \lambda_i(\ell) \neq 0\} & \text{if } \ell \in \mathbf{N}. \end{cases}$$

Note that for every $\ell \in \mathbf{N}$, we have

$$p^{\rho(\ell)-1} \leq \ell < p^{\rho(\ell)}.$$

For $L = (\ell_1, \ldots, \ell_n) \in \mathbf{N}_0^n$, we now let

$$\kappa(L) = \sum_{j=1}^n \kappa(\ell_j) \quad \text{and} \quad \rho(L) = \sum_{j=1}^n \rho(\ell_j). \tag{26}$$

It is easy to check that $\kappa(L) = \rho(L) = 0$ if and only if $L = 0$. One can also easily check the triangle inequalities for both weights. These give rise to metrics (or distances) on the vector space $\ell \in \mathbf{N}_0^n$.

These metrics are intimately related to those defined in Section 2 on elements in $\mathbf{Q}^n(p^s)$. It is not difficult to see that the mapping (24) is an isomorphism that preserves the metrics κ and ρ. More precisely, for every $X \in \mathbf{Q}^n(p^s)$, we have

$$\kappa(X) = \kappa(\theta(X)) \quad \text{and} \quad \rho(X) = \rho(\theta(X)). \tag{27}$$

7 Approximation of the discrepancy function

For any $Y = (y_1, \ldots, y_n) \in U^n$, we consider the characteristic function $\chi(Y, X)$ of the rectangular box $B_Y = [0, y_1) \times \ldots \times [0, y_n)$, so that

$$\chi(Y, X) = \begin{cases} 1 & \text{if } X \in B_Y, \\ 0 & \text{if } X \notin B_Y. \end{cases}$$

It is clear that if $X = (x_1, \ldots, x_n)$, then

$$\chi(Y, X) = \prod_{j=1}^n \chi(y_j, x_j),$$

where for every $j = 1, \dots, n$,

$$\chi(y_j, x_j) = \begin{cases} 1 & \text{if } x_j \in [0, y_j), \\ 0 & \text{if } x_j \notin [0, y_j). \end{cases}$$

For any linear distribution $D \subset \mathbf{Q}^n(p^s)$ of p^s points, we have

$$\mathcal{L}[D; Y] = \sum_{X \in D} \chi(Y, X) - p^s y_1 \dots y_n.$$

The function $\chi(y, x)$ has a Fourier–Walsh expansion of the form

$$\chi(y, x) \simeq \sum_{\ell=0}^{\infty} \widetilde{\chi}_\ell(y) \overline{w_\ell(x)},$$

where for every $\ell \in \mathbf{N}_0$, the Fourier–Walsh coefficients are defined by

$$\widetilde{\chi}_\ell(y) = \int_0^y w_\ell(x)\, \mathrm{d}x.$$

In particular, we have $\widetilde{\chi}_0(y) = y$.

Following [3], for given $s \in \mathbf{N}_0$, we approximate $\chi(y, x)$ by the truncated series

$$\chi_s(y, x) = \sum_{\ell=0}^{p^s-1} \widetilde{\chi}_\ell(y) \overline{w_\ell(x)}, \tag{28}$$

the characteristic function $\chi(Y, X)$ by the product

$$\chi_s(Y, X) = \prod_{j=1}^{n} \chi_s(y_j, x_j), \tag{29}$$

and the discrepancy function $\mathcal{L}[D; Y]$ by

$$\mathcal{M}[D; Y] = \sum_{X \in D} \chi_s(Y, X) - p^s y_1 \dots y_n. \tag{30}$$

The following estimate, essentially Lemma 6A of [3], gives a bound for the error of this approximation process.

Lemma 7.1. *Suppose that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ satisfying $\rho(D^\perp) \geq s + 1$. Then for every $Y \in U^n$, we have $|\mathcal{L}[D; Y] - \mathcal{M}[D; Y]| \leq n$.*

For every $L = (\ell_1, \dots, \ell_n) \in \mathbf{N}_0^n$ and $Y = (y_1, \dots, y_n) \in U^n$, write

$$\widetilde{\chi}_L(Y) = \widetilde{\chi}_{\ell_1}(y_1) \dots \widetilde{\chi}_{\ell_n}(y_n). \tag{31}$$

In view of (28)–(31), (21) and Lemma 5.1, we have

$$\begin{aligned}\mathcal{M}[D;Y] &= \sum_{X\in D}\sum_{L\in\mathbf{N}_0^n(p^s)} \widetilde{\chi}_L(Y)\,\overline{W_L(X)} - p^s\widetilde{\chi}_0(y_1)\dots\widetilde{\chi}_0(y_n)\\ &= \sum_{L\in\mathbf{N}_0^n(p^s)}\left(\sum_{X\in D}\overline{W_L(X)}\right)\widetilde{\chi}_L(Y) - p^s\widetilde{\chi}_0(Y)\\ &= p^s\sum_{L\in\theta(D^\perp)\setminus\{0\}}\widetilde{\chi}_L(Y). \end{aligned} \tag{32}$$

The result below follows immediately.

Lemma 7.2. *Suppose that $D\subset\mathbf{Q}^n(p^s)$ is a linear distribution of p^s points. Suppose further that for any distinct $L', L''\in\theta(D^\perp)\setminus\{0\}$, the functions $\widetilde{\chi}_{L'}$ and $\widetilde{\chi}_{L''}$ are orthogonal to each other. Then*

$$\int_{U^n}|\mathcal{M}[D;Y]|^2\,\mathrm{d}Y = p^{2s}\sum_{L\in\theta(D^\perp)\setminus\{0\}}\int_{U^n}|\widetilde{\chi}_L(Y)|^2\,\mathrm{d}Y. \tag{33}$$

Next, we consider digit shifts.

Lemma 7.3. *Suppose that $D\subset\mathbf{Q}^n(p^s)$ is a linear distribution of p^s points. Then*

$$\frac{1}{p^{ns}}\sum_{T\in\mathbf{Q}^n(p^s)}\int_{U^n}|\mathcal{M}[D\oplus T;Y]|^2\,\mathrm{d}Y = p^{2s}\sum_{L\in\theta(D^\perp)\setminus\{0\}}\int_{U^n}|\widetilde{\chi}_L(Y)|^2\,\mathrm{d}Y. \tag{34}$$

Proof. For every fixed $T\in\mathbf{Q}^n(p^s)$, the coset $D\oplus T$, obtained by applying the same digit shift to every point of D and given by (11), satisfies

$$\begin{aligned}\mathcal{M}[D\oplus T;Y] &= \sum_{X\in D}\sum_{L\in\mathbf{N}_0^n(p^s)}\widetilde{\chi}_L(Y)\,\overline{W_L(X\oplus T)} - p^s\widetilde{\chi}_0(y_1)\dots\widetilde{\chi}_0(y_n)\\ &= \sum_{L\in\mathbf{N}_0^n(p^s)}\overline{W_L(T)}\left(\sum_{X\in D}\overline{W_L(X)}\right)\widetilde{\chi}_L(Y) - p^s\widetilde{\chi}_0(Y)\\ &= p^s\sum_{L\in\theta(D^\perp)\setminus\{0\}}\overline{W_L(T)}\,\widetilde{\chi}_L(Y), \end{aligned}$$

in view of (23). It follows that

$$\begin{aligned}
&\sum_{T\in\mathbf{Q}^n(p^s)} |\mathcal{M}[D\oplus T;Y]|^2\\
&= p^{2s}\sum_{T\in\mathbf{Q}^n(p^s)}\left|\sum_{L\in\theta(D^\perp)\setminus\{0\}}\overline{W_L(T)}\,\widetilde{\chi}_L(Y)\right|^2\\
&= p^{2s}\sum_{T\in\mathbf{Q}^n(p^s)}\sum_{L',L''\in\theta(D^\perp)\setminus\{0\}}\overline{W_{L'}(T)}\,W_{L''}(T)\,\widetilde{\chi}_{L'}(Y)\,\overline{\widetilde{\chi}_{L''}(Y)}\\
&= p^{2s}\sum_{L',L''\in\theta(D^\perp)\setminus\{0\}}\left(\sum_{T\in\mathbf{Q}^n(p^s)}\overline{W_{L'}(T)}\,W_{L''}(T)\right)\widetilde{\chi}_{L'}(Y)\,\overline{\widetilde{\chi}_{L''}(Y)}\\
&= p^{ns}p^{2s}\sum_{L\in\theta(D^\perp)\setminus\{0\}}|\widetilde{\chi}_L(Y)|^2,
\end{aligned}$$

in view of Lemma 5.2. The identity (34) then follows immediately on integrating over $Y\in U^n$. □

Note that the right hand sides of (33) and (34) are identical. The former is a consequence of the orthogonality of the Fourier–Walsh coefficients, while the latter is a consequence of the orthogonality condition (25) brought into play by the digit shifts. Noting (31), we see that to progress further, we clearly need to study the integral

$$\int_{U^n}|\widetilde{\chi}_L(Y)|^2\,\mathrm{d}Y=\prod_{j=1}^n\int_U|\widetilde{\chi}_{\ell_j}(y_j)|^2\,\mathrm{d}y_j. \tag{35}$$

Lemma 7.4. *We have*

$$\int_U|\widetilde{\chi}_0(y)|^2\,\mathrm{d}y=\frac{1}{4}+\frac{1}{4(p^2-1)}\sum_{j=1}^{p-1}\csc^2\frac{\pi j}{p}. \tag{36}$$

Furthermore, for every $\ell\in\mathbf{N}$, we have

$$\int_U|\widetilde{\chi}_\ell(y)|^2\,\mathrm{d}y=p^{-2\rho(\ell)}\left(\frac{1}{2}\csc^2\frac{\pi\lambda(\ell)}{p}-\frac{1}{4}+\frac{1}{4(p^2-1)}\sum_{j=1}^{p-1}\csc^2\frac{\pi j}{p}\right), \tag{37}$$

where $\lambda(\ell)=\lambda_{\rho(\ell)}(\ell)$ denotes the leading coefficient in the p-ary expansion (15) *of ℓ.*

Proof. We have the Fine–Price formula, that for every $\ell\in\mathbf{N}_0$,

$$\widetilde{\chi}_\ell(y)=p^{-\rho(\ell)}u_\ell(y), \tag{38}$$

where

$$u_0(y)=\frac{1}{2}w_0(y)+\sum_{i=1}^{\infty}p^{-i}\sum_{j=1}^{p-1}\zeta^j(1-\zeta^j)^{-1}w_{jp^{i-1}}(y), \tag{39}$$

and where for every $\ell \in \mathbf{N}$,

$$u_\ell(y) = (1-\zeta^{\lambda(\ell)})^{-1} w_{\tau(\ell)}(y) + \left(\frac{1}{2} - (1-\zeta^{\lambda(\ell)})^{-1}\right) w_\ell(y) + \sum_{i=1}^{\infty} p^{-i} \sum_{j=1}^{p-1} \zeta^j (1-\zeta^j)^{-1} w_{\ell+jp^{\rho(\ell)+i-1}}(y). \tag{40}$$

Here $\tau(\ell) = \ell - \lambda(\ell) p^{\rho(\ell)-1}$, and $\zeta = \mathrm{e}^{2\pi \mathrm{i}/p}$ is a primitive p-th root of unity. For details, see Fine [6] and Price [10]. The right hand side of (40) is a linear combination of distinct Walsh functions. It follows that for every $\ell \in \mathbf{N}$, we have

$$\begin{aligned}\int_U |u_\ell(y)|^2 \,\mathrm{d}y &= \frac{1}{(1-\zeta^{\lambda(\ell)})(1-\zeta^{-\lambda(\ell)})} + \left(\frac{1}{2} - \frac{1}{1-\zeta^{\lambda(\ell)}}\right)\left(\frac{1}{2} - \frac{1}{1-\zeta^{-\lambda(\ell)}}\right) \\ &\quad + \sum_{i=1}^{\infty} p^{-2i} \sum_{j=1}^{p-1} |1-\zeta^j|^{-2} \\ &= 2|1-\zeta^{\lambda(\ell)}|^{-2} - \frac{1}{4} + \frac{1}{p^2-1} \sum_{j=1}^{p-1} |1-\zeta^j|^{-2}. \end{aligned} \tag{41}$$

The identity (37) follows on combining (38) and (41) with the observation

$$|1-\zeta^j|^2 = \left(1 - \cos\frac{2\pi j}{p}\right)^2 + \sin^2\frac{2\pi j}{p} = 4\sin^2\frac{\pi j}{p}. \tag{42}$$

Similarly, we have

$$\int_U |u_0(y)|^2 \,\mathrm{d}y = \frac{1}{4} + \sum_{i=1}^{\infty} p^{-2i} \sum_{j=1}^{p-1} |1-\zeta^j|^{-2} = \frac{1}{4} + \frac{1}{p^2-1} \sum_{j=1}^{p-1} |1-\zeta^j|^{-2}. \tag{43}$$

The identity (36) follows on combining (38), (42) and (43). □

Lemma 7.5. *For every $L \in \mathbf{N}_0^n$, we have*

$$\int_{U^n} |\widetilde{\chi}_L(Y)|^2 \,\mathrm{d}Y \le \frac{p^{2n-2\rho(L)}}{4^n}.$$

Proof. In view of (35), it suffices to show that for every $\ell \in \mathbf{N}_0$, we have

$$\int_U |\widetilde{\chi}_\ell(y)|^2 \,\mathrm{d}y \le \frac{p^{2-2\rho(\ell)}}{4}.$$

Suppose first of all that $\ell \ne 0$. Then using the inequality that

$$\csc^2\frac{\pi j}{p} \le \frac{p^2}{4} \quad \text{for every } j = 1, \ldots, p-1,$$

we see from (37) that

$$\int_U |\widetilde{\chi}_\ell(y)|^2 \, \mathrm{d}y \le p^{-2\rho(\ell)} \left(\frac{p^2}{8} + \frac{1}{4} + \frac{p^2(p-1)}{16(p^2-1)} \right) \le \frac{p^{2-2\rho(\ell)}}{4}.$$

On the other hand, it follows similarly from (36) that

$$\int_U |\widetilde{\chi}_0(y)|^2 \, \mathrm{d}y \le \frac{1}{4} + \frac{p^2(p-1)}{16(p^2-1)} \le \frac{p^2}{4} = \frac{p^{2-2\rho(0)}}{4}.$$

□

Here we take a digression and make a brief comment on the case $p = 2$, where it is easy to show that

$$\int_{U^n} |\widetilde{\chi}_L(Y)|^2 \, \mathrm{d}Y = \frac{4^{-\rho(L)}}{3^n}.$$

Suppose that D is a linear distribution of 2^s points. Then it follows immediately from Lemma 7.3 that

$$\frac{1}{2^{ns}} \sum_{T \in \mathbf{Q}^n(2^s)} \int_{U^n} |\mathcal{M}[D \oplus T; Y]|^2 \, \mathrm{d}Y = \frac{4^s}{3^n} \sum_{L \in \theta(D^\perp) \setminus \{0\}} 4^{-\rho(L)}.$$

Furthermore, it follows immediately from Lemma 7.2 that

$$\int_{U^n} |\mathcal{M}[D; Y]|^2 \, \mathrm{d}Y = \frac{4^s}{3^n} \sum_{L \in \theta(D^\perp) \setminus \{0\}} 4^{-\rho(L)}, \tag{44}$$

provided that the functions $\widetilde{\chi}_{L'}$ and $\widetilde{\chi}_{L''}$, where $L', L'' \in \theta(D^\perp) \setminus \{0\}$, are orthogonal to each other. The formula (44) shows that the L_2-norm of the approximation $M[D; Y]$ coincides with a Rosenbloom–Tsfasman enumerator for the subspace $D^\perp$.

We now return to our main discussion. The following estimate is given by Lemma 6D of [3].

Lemma 7.6. *Suppose that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ satisfying $\rho(D^\perp) \ge s + 1$. Then*

$$\sum_{L \in \theta(D^\perp) \setminus \{0\}} p^{2s - 2\rho(L)} < (s+1)^{n-1}.$$

Combining Lemmas 7.5 and 7.6, we conclude that

$$p^{2s} \sum_{L \in \theta(D^\perp) \setminus \{0\}} \int_{U^n} |\widetilde{\chi}_L(Y)|^2 \, \mathrm{d}Y \le \frac{p^{2n}}{4^n} (s+1)^{n-1}. \tag{45}$$

8 Deduction of Theorem 5

Suppose that $p \ge n - 1$ is a prime. Suppose further that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ that satisfies

$\rho(D^\perp) \ge s+1$. Combining Lemma 7.3 and the inequality (45), we conclude that

$$\frac{1}{p^{ns}} \sum_{T \in \mathbf{Q}^n(p^s)} \int_{U^n} |\mathcal{M}[D \oplus T; Y]|^2 \, \mathrm{d}Y \le \frac{p^{2n}}{4^n}(s+1)^{n-1}.$$

It follows that there exists a digit shift $T \in \mathbf{Q}^n(p^s)$ such that

$$\int_{U^n} |\mathcal{M}[D \oplus T; Y]|^2 \, \mathrm{d}Y \le \frac{p^{2n}}{4^n}(s+1)^{n-1}.$$

It is not too difficult to check that the conclusion of Lemma 7.1 remains valid for this coset $D \oplus T$, so that

$$\begin{aligned} \int_{U^n} |\mathcal{L}[D \oplus T; Y]|^2 \, \mathrm{d}Y &\le 2 \int_{U^n} |\mathcal{M}[D \oplus T; Y]|^2 \, \mathrm{d}Y + 2n^2 \\ &\le \frac{2p^{2n}}{4^n}(s+1)^{n-1} + 2n^2 \le \frac{4p^{2n}}{4^n}(s+1)^{n-1}, \end{aligned} \tag{46}$$

where the last inequality is valid with the possible exception of the cases

$$\begin{cases} s = 0, \\ s = 1, \ p = 2, \ n = 2, \\ s = 1, \ p = 2, \ n = 3, \\ s = 2, \ p = 2, \ n = 2. \end{cases} \tag{47}$$

The inequality (12) follows immediately from the inequality (46) on taking square roots. On the other hand, the inequality (12) holds trivially for each of the first three exceptional cases in (47). For the remaining case, we simply note that the uniformity of the linear distribution D implies that $|\mathcal{L}[D \oplus T; Y]| \le 3$ for every $Y \in U^2$, so that the inequality (12) follows again. This completes the proof of Theorem 5.

9 Deduction of Theorems 3 and 4

The following crucial orthogonality relationship arises from the very recent work of Skriganov [18] on L_q-discrepancy.

Lemma 9.1. *Suppose that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ satisfying $\kappa(D^\perp) \ge 2n+1$. Then for any distinct $L', L'' \in \theta(D^\perp) \setminus \{0\}$, the functions $\widetilde{\chi}_{L'}$ and $\widetilde{\chi}_{L''}$ are orthogonal to each other.*

Suppose that $p \ge 2n^2$ is a prime. Suppose further that $D \subset \mathbf{Q}^n(p^s)$ is a linear distribution of p^s points, with dual linear distribution $D^\perp \subset \mathbf{Q}^n(p^s)$ that satisfies

$$\kappa(D^\perp) \ge 2n+1 \quad \text{and} \quad \rho(D^\perp) \ge s+1.$$

The assertions (8) and (9) of Theorem 4 follow immediately from Lemmas 7.1, 7.2, 9.1 and 7.4, together with the identity (35). The assertion (10) of Theorem 4 follows as a simple consequence of the inequality (8).

Furthermore, combining Lemmas 9.1 and 7.2 with the inequality (45), we have

$$\int_{U^n} |\mathcal{M}[D; Y]|^2 \, \mathrm{d}Y \le \frac{p^{2n}}{4^n}(s+1)^{n-1}.$$

It then follows from Lemma 7.1 that

$$\int_{U^n} |\mathcal{L}[D; Y]|^2 \, \mathrm{d}Y \le 2 \int_{U^n} |\mathcal{M}[D; Y]|^2 \, \mathrm{d}Y + 2n^2$$

$$\le \frac{2p^{2n}}{4^n}(s+1)^{n-1} + 2n^2 \le \frac{4p^{2n}}{4^n}(s+1)^{n-1}.$$

The inequality (7) follows immediately on taking square roots. This completes the proof of Theorem 3.

We complete this paper by giving the very short proof of Lemma 9.1. Note first that a consequence of (31) is the identity

$$\int_{U^n} \widetilde{\chi}_{L'}(Y) \overline{\widetilde{\chi}_{L''}(Y)} \, \mathrm{d}Y = \prod_{j=1}^{n} \int_{U} \widetilde{\chi}_{\ell'_j}(y_j) \overline{\widetilde{\chi}_{\ell''_j}(y_j)} \, \mathrm{d}y_j.$$

On the other hand, the condition $\kappa(D^{\perp}) \ge 2n+1$ and the relationship (27) imply that for any distinct $L', L'' \in \theta(D^{\perp}) \setminus \{0\}$, we must have $\kappa(L' \ominus L'') \ge 2n+1$. It follows from (26) and the pigeonhole principle that $\kappa(\ell'_j \ominus \ell''_j) \ge 3$ for some $j = 1, \ldots, k$. Hence Lemma 9.1 is an immediate consequence of the following one-dimensional result.

Lemma 9.2. *Suppose that $\ell', \ell'' \in \mathbf{N}_0$ and $\kappa(\ell' \ominus \ell'') \ge 3$. Then $\widetilde{\chi}_{\ell'}$ and $\widetilde{\chi}_{\ell''}$ are orthogonal to each other.*

Proof. The Fine–Price formula (38)–(40) can be rewritten in the following form. For every $\ell \in \mathbf{N}_0$, we have

$$\widetilde{\chi}_{\ell}(y) = p^{-\rho(\ell)} w_{\ell}(y) v_{\ell}(y), \tag{48}$$

where

$$v_0(y) = \frac{1}{2} w_0(y) + \sum_{i=1}^{\infty} p^{-i} \sum_{j=1}^{p-1} \zeta^j (1-\zeta^j)^{-1} w_{jp^{i-1}}(y), \tag{49}$$

and where for every $\ell \in \mathbf{N}$,

$$v_{\ell}(y) = (1-\zeta^{\lambda(\ell)})^{-1} w_{\lambda(\ell)p^{\rho(\ell)-1}}(y) + \left(\frac{1}{2} - (1-\zeta^{\lambda(\ell)})^{-1}\right) w_0(y)$$

$$+ \sum_{i=1}^{\infty} p^{-i} \sum_{j=1}^{p-1} \zeta^j (1-\zeta^j)^{-1} w_{jp^{\rho(\ell)+i-1}}(y). \tag{50}$$

Note first of all from (49) and (50) that for every $\ell \in \mathbf{N}_0$, there exists a set $\mathcal{K} = \mathcal{K}(\ell)$ of nonnegative integers, depending only on ℓ, such that

$$v_{\ell}(y) = \sum_{k \in \mathcal{K}} c_k w_k(y),$$

where for every $k \in \mathcal{K}$, the p-ary expansion of k has at most one nonzero coefficient. Suppose now that $\ell', \ell'' \in \mathbf{N}_0$ are distinct. Then there exist two sets $\mathcal{K}' = \mathcal{K}'(\ell')$ and $\mathcal{K}'' = \mathcal{K}''(\ell'')$ of nonnegative integers such that

$$v_{\ell'}(y)\,\overline{v_{\ell''}(y)} = \sum_{k' \in \mathcal{K}'} \sum_{k'' \in \mathcal{K}''} c_{k'} \overline{c_{k''}}\, w_{k' \ominus k''}(y),$$

where for every $k' \in \mathcal{K}'$ and $k'' \in \mathcal{K}''$, the p-ary expansion of $k' \ominus k''$ has at most two nonzero coefficients. Combining this with (48), we conclude that

$$\begin{aligned} \widetilde{\chi}_{\ell'}(y)\,\overline{\widetilde{\chi}_{\ell''}(y)} &= p^{-\rho(\ell')-\rho(\ell'')} w_{\ell' \ominus \ell''}(y) \sum_{k' \in \mathcal{K}'} \sum_{k'' \in \mathcal{K}''} c_{k'} \overline{c_{k''}}\, w_{k' \ominus k''}(y) \\ &= p^{-\rho(\ell')-\rho(\ell'')} \sum_{k' \in \mathcal{K}'} \sum_{k'' \in \mathcal{K}''} c_{k'} \overline{c_{k''}}\, w_{\ell' \ominus \ell'' \oplus k' \ominus k''}(y). \end{aligned} \tag{51}$$

On the other hand, the condition $\kappa(\ell' \ominus \ell'') \geq 3$ ensures that the p-ary expansion of $\ell' \ominus \ell''$ has at least three nonzero coefficients. It follows that for every $k' \in \mathcal{K}'$ and $k'' \in \mathcal{K}''$, the p-ary expansion of $\ell' \ominus \ell'' \oplus k' \ominus k''$ has at least one nonzero coefficient, so that $\ell' \ominus \ell'' \oplus k' \ominus k''$ is nonzero. It follows from (51) and (20) that

$$\begin{aligned} &\int_U \widetilde{\chi}_{\ell'}(y)\,\overline{\widetilde{\chi}_{\ell''}(y)}\,\mathrm{d}y \\ &\quad = p^{-\rho(\ell')-\rho(\ell'')} \sum_{k' \in \mathcal{K}'} \sum_{k'' \in \mathcal{K}''} c_{k'} \overline{c_{k''}} \int_U w_{\ell' \ominus \ell'' \oplus k' \ominus k''}(y)\,\mathrm{d}y = 0. \end{aligned}$$

□

Acknowledgments. The research of the second author has been supported by RFFI Project No. 02-01-00086 and INTAS Grant No. 00-429.

References

1. Chen, W.W.L.: On irregularities of distribution. *Mathematika* **27**, 153–170 (1980)
2. Chen, W.W.L.: On irregularities of distribution II. *Q. J. Math. Oxf.* **34**, 257–279 (1983)
3. Chen, W.W.L., Skriganov, M.M.: Explicit constructions in the classical mean squares problem in irregularities of point distribution. *J. Reine Angew. Math.* **545**, 67–95 (2002)
4. Dobrovol'skiĭ, N.M.: An effective proof of Roth's theorem on quadratic dispersion. *Usp. Mat. Nauk* **39**, 155–156 (1984); *Russ. Math. Surv.* **39**, 117–118 (1984)
5. Faure, H.: Discrépance de suites associées à un système de numération (en dimension s). *Acta Arith.* **41**, 337–351 (1982)
6. Fine, N.J.: On the Walsh functions. *Trans. Am. Math. Soc.* **65**, 373–414 (1949)
7. Frolov, K.K.: An upper bound for the discrepancy in the L_p-metric. *Dokl. Akad. Nauk SSSR* **252**, 805–807 (1980)
8. Golubov, B.I., Efimov, A.V., Skvorčov, V.A.: *The Walsh Series and Transformations: Theory and Applications*. Kluwer, Dordrecht (1991)
9. Hewitt, E., Ross, K.A.: *Abstract Harmonic Analysis*, vol. 1. Springer, Heidelberg (1963)
10. Price, J.J.: Certain groups of orthonormal step functions. *Can. J. Math.* **9**, 413–425 (1957)
11. Rosenbloom, M.Yu., Tsfasman, M.A.: Codes in the m-metric. *Probl. Peredachi Inf.* **33**, 55–63 (1997); *Probl. Inf. Transm.* **33**, 45–52 (1997)
12. Roth, K.F.: On irregularities of distribution. *Mathematika* **11**, 73–79 (1954)
13. Roth, K.F.: On irregularities of distribution IV. *Acta Arith.* **37**, 67–75 (1980)

14. Schipp, F., Wade, W.R., Simon, P.: *Walsh Series: An Introduction to Dyadic Harmonic Analysis*. Hilger, Bristol (1990)
15. Skriganov, M.M.: Lattices in algebraic number fields and uniform distribution modulo 1. *Algebra Anal.* **1**, 207–228 (1989); *Leningr. Math. J.* **1**, 535–558 (1990)
16. Skriganov, M.M.: Constructions of uniform distributions in terms of geometry of numbers. *Algebra Anal.* **6**, 200–230 (1994); *St. Petersbg. Math. J.* **6**, 635–664 (1995)
17. Skriganov, M.M.: Coding theory and uniform distributions. *Algebra Anal.* **13**, 191–239 (2001); *St. Petersbg. Math. J.* **13**, 301–337 (2002)
18. Skriganov, M.M.: Harmonic analysis on totally disconnected groups and irregularities of point distributions. *J. Reine Angew. Math.* **600**, 25–49 (2006)