NOTE ON IRREGULARITIES OF DISTRIBUTION II

J. BECK *and* W. W. L. CHEN

[Received 2 March 1989]

1. *Introduction*

Suppose that $\mathcal{P}$ is a distribution of N points in the unit torus $U^L = [0, 1)^2$, where $L \geqslant 1$. For every $\mathbf{y} = (y_1, \ldots, y_L) \in U^L$, let

$$B(\mathbf{y}) = [0, y_1) \times \ldots \times [0, y_L),$$

and let

$$Z_L[\mathcal{P}; B(\mathbf{y})] = \#(\mathcal{P} \cap B(\mathbf{y})),$$

where $\#\mathcal{S}$ denotes the cardinality of the set $\mathcal{S}$. We are interested in the discrepancy function

$$D_L[\mathcal{P}; B(\mathbf{y})] = Z_L[\mathcal{P}; B(\mathbf{y})] - N\mu_L(B(\mathbf{y})),$$

where μ_L denotes the usual volume in U^L. The case where $L = 1$ is trivial. For $L \geqslant 2$, the following results are well known.

THEOREM 1A (Roth [**10**]). *Suppose that $\mathcal{P}$ is a distribution of N points in U^L. Then*

$$\int_{U^L} |D_L[\mathcal{P}; B(\mathbf{y})]|^2 \, d\mathbf{y} \gg_L (\log N)^{L-1}.$$

THEOREM 1B (Roth [**11**]). *For every natural number $N \geqslant 2$, there exists a distribution $\mathcal{P}$ of N points in U^L such that*

$$\int_{U^L} |D_L[\mathcal{P}; B(\mathbf{y})]|^2 \, d\mathbf{y} \ll_L (\log N)^{L-1}.$$

Note that Theorems 1A and 1B remain true in the trivial case $L = 1$.

Suppose now that $\mathcal{P}$ is a distribution of N points in the unit torus $U^K = [0, 1)^K$, where $K \geqslant 2$. Let A be a compact and convex body in U^K. For any real number $\lambda \in (0, 1]$, any proper orthogonal transformation τ in $\mathbb{R}^K$ and any vector $\mathbf{u} \in U^K$, let

$$A(\lambda, \tau, \mathbf{u}) = \{\tau(\lambda \mathbf{x}) + \mathbf{u}: \ \mathbf{x} \in A\}$$

(note that $A(\lambda, \tau, \mathbf{u})$ and A are similar to each other), and let

$$Z_K[\mathcal{P}; A(\lambda, \tau, \mathbf{u})] = \#(\mathcal{P} \cap A(\lambda, \tau, \mathbf{u})).$$

We are interested in the discrepancy function

$$D_K[\mathcal{P}; A(\lambda, \tau, \mathbf{u})] = Z_K[\mathcal{P}; A(\lambda, \tau, \mathbf{u})] - N\mu_K(A(\lambda, \tau, \mathbf{u})),$$

where μ_K denotes the usual volume in U^K. Corresponding to Theorem 1A, we have the following result. Let $\mathcal{T}$ be the group of all proper orthogonal transformations in $\mathbb{R}^K$, and let $d\tau$ be the volume element of the invariant measure on $\mathcal{T}$, normalized such that $\int_{\mathcal{T}} d\tau = 1$.

A.M.S. (*1980*) *subject classification*: 11K38.

Proc. London Math. Soc. (3) 61 (1990) 251–272.

THEOREM 2A (Beck [1]). *Suppose that $\mathcal{P}$ is a distribution of N points in U^K, and that A is a compact and convex body in U^K. Suppose further that $r(A) \geqslant N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of A. Then*

$$\int_0^1 \int_{\mathcal{T}} \int_{U^K} |D_K[\mathcal{P}; A(\lambda, \tau, \mathbf{u})]|^2 \, d\mathbf{u} \, d\tau \, d\lambda \gg_A N^{1-1/K}.$$

We comment here that special cases of Theorem 2A are also discussed by Montgomery in [9]. On the other hand, Theorem 2A is sharp. The following analogue of Theorem 1B can be deduced using ideas of Beck and Chen [2].

THEOREM 2B. *Suppose that A is a compact and convex body in U^K. Then for every natural number N, there exists a distribution $\mathcal{P}$ of N points in U^K such that*

$$\int_0^1 \int_{\mathcal{T}} \int_{U^K} |D_K[\mathcal{P}; A(\lambda, \tau, \mathbf{u})]|^2 \, d\mathbf{u} \, d\tau \, d\lambda \ll_A N^{1-1/K}.$$

In this paper, we investigate a combination of these two problems. More precisely, suppose that $\mathcal{P}$ is a distribution of N points in the unit torus U^{K+L}, where $K \geqslant 2$ and $L \geqslant 1$. Let A be a compact and convex body in U^K. For any real number $\lambda \in (0, 1]$, any proper orthogonal transformation τ in $\mathbb{R}^K$, any vectors $\mathbf{u} \in U^K$ and $\mathbf{y} \in U^K$, we consider the cartesian product $A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y})$, where $A(\lambda, \tau, \mathbf{u}) \in U^L$ and $B(\mathbf{y}) \in U^L$ are defined as before, and let

$$Z[\mathcal{P}; A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y})] = \#(\mathcal{P} \cap (A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y}))).$$

We are interested in the discrepancy function

$$D[\mathcal{P}; A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y})] = Z[\mathcal{P}; A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y})] - N\mu_K(A(\lambda, \tau, \mathbf{u}))\mu_L(B(\mathbf{y})).$$

A simple corollary of Theorem 2A is the following lower bound result.

THEOREM 3A. *Suppose that $\mathcal{P}$ is a distribution of N points in U^{K+L}, and that A is a compact and convex body in U^K. Suppose further that $r(A) \geqslant N^{-1/K}$, where $r(A)$ denotes the radius of the largest inscribed ball of A. Then*

$$\int_0^1 \int_{\mathcal{T}} \int_{U^K} \int_{U^L} |D[\mathcal{P}; A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y})]|^2 \, d\mathbf{y} \, d\mathbf{u} \, d\tau \, d\lambda \gg_{A,L} N^{1-1/K}.$$

The argument of Beck and Chen in [2] can be adapted to show that Theorem 3A is sharp in the case where $L = 1$. The purpose of this paper is to investigate the cases where $L \geqslant 2$. We prove the following complementary result.

THEOREM 3B. *Suppose that A is a compact and convex body in U^K. Then for every natural number N, there exists a distribution $\mathcal{P}$ of N points in U^{K+L} such that*

$$\int_0^1 \int_{\mathcal{T}} \int_{U^K} \int_{U^L} |D[\mathcal{P}; A(\lambda, \tau, \mathbf{u}) \times B(\mathbf{y})]|^2 \, d\mathbf{y} \, d\mathbf{u} \, d\tau \, d\lambda \ll_{A,L} N^{1-1/K}.$$

In other words, we prove that Theorem 3A is sharp, apart from the value of the implicit constant. Note also that the order of magnitude of the estimates is independent of L.

For further discussion on irregularities of distribution, see Schmidt [12] and Beck and Chen [3].

2. *The basic idea*

For convenience of notation, we shall in fact prove Theorem 3B in the case of $U^{K+(L+1)}$. Let A be given and fixed. Given any natural number N, we shall show that there exists a sequence $\mathbf{p}_0, \ldots, \mathbf{p}_{N-1}$ of N points in U^{K+L} such that

$$\frac{1}{N}\sum_{M=1}^{N}\int_0^1\int_{\mathscr{T}}\int_{U^K}\int_{U^L}|D[\mathscr{P}_M; A(\lambda, \tau, \mathbf{u})\times B(\mathbf{y})]|^2\,d\mathbf{y}\,d\mathbf{u}\,d\tau\,d\lambda \ll_{A,L} N^{1-1/K}, \quad (1)$$

where $\mathscr{P}_M = \{\mathbf{p}_0, \ldots, \mathbf{p}_{M-1}\}$ for $1 \leq M \leq N$. Theorem 3B in the case of $U^{K+(L+1)}$ follows easily.

We shall in fact construct a sequence of more than N points in U^{K+L} and use only the first N terms of this sequence. The main ingredient in the construction of this sequence in U^{K+L} is the Chinese remainder theorem. This not only makes it possible for the determination of the first K coordinates of the points of the sequence to be carried out independently of the determination of the last L coordinates of these points, but also enables us to treat the discrepancy arising from $A(\lambda, \tau, \mathbf{u})$ quite separately from the discrepancy arising from $B(\mathbf{y})$. Furthermore, it ensures that important properties of the sequence are also present in many subsequences that arise from our argument.

3. *The sequence: general discussion*

Let h be a natural number, and let $p_1, \ldots, p_L$ be the first L odd primes.

For every $p = 2, p_1, \ldots, p_L$, for every $s = 0, 1, \ldots, h$ and for every $c \in \mathbb{Z}$, let

$$I(p, s, c) = [cp^{-s}, (c+1)p^{-s}). \quad (2)$$

In other words, $I(p, s, c)$ is an interval of length p^{-s} and whose endpoints are consecutive integer multiples of p^{-s}.

We shall construct an infinite sequence of points $\mathbf{p}_0, \mathbf{p}_1, \mathbf{p}_2, \ldots$ in U^{K+L} such that the following is satisfied. For every $s_0, s_1, \ldots, s_L \in \{0, 1, \ldots, h\}$, every set of the form

$$I(2, s_0, a_1)\times\ldots\times I(2, s_0, a_K)\times I(p_1, s_1, b_1)\times\ldots\times I(p_L, s_L, b_L)$$

in U^{K+L}, where $a_1, \ldots, a_K, b_1, \ldots, b_L \in \mathbb{Z}$, contains exactly one point of

$$\{\mathbf{p}_n:\ c2^{Ks_0}p_1^{s_1}\ldots p_L^{s_L} \leq n < (c+1)2^{Ks_0}p_1^{s_1}\ldots p_L^{s_L}\},$$

where c is any non-negative integer.

The construction of such a sequence involves ideas in combinatorics and poses no real difficulty. However, such a sequence alone is insufficient to give a proof of Theorem 3B. As Beck and Chen did in [2], we appeal to tools in probability theory. Note that the situation here is much more complicated than that in [2]. In fact, we need to apply probabilistic arguments in two quite different ways. One of these, to deal with the discrepancy arising from $A(\lambda, \tau, \mathbf{u})$, is essentially similar to the probabilistic arguments in [2]. However, to deal with the discrepancy arising from $B(\mathbf{y})$, we appeal to a probabilistic argument first introduced by Chen [5].

Needless to say, our combinatorial construction has to be carried out in such a way that our probabilistic arguments can be implemented with ease.

For every non-negative integer n, let

$$\mathbf{p}_n = (\mathbf{q}_n, \mathbf{y}_n) \in U^{K+L},$$

where $\mathbf{q}_n \in U^K$ and $\mathbf{y}_n \in U^L$. We shall discuss the sequence $\mathbf{q}_n$ in §§ 4–6 and the sequence $\mathbf{y}_n$ in §§ 7–8.

4. *A combinatorial approach*

For every integer s satisfying $1 \leqslant s \leqslant h$, integers $\tau_1, \ldots, \tau_{s-1} \in \{0, 1, \ldots, 2^K - 1\}$ and vectors $\mathbf{a}_1, \ldots, \mathbf{a}_{s-1} \in \{0, 1\}^K$, let

$$G[\tau_1, \ldots, \tau_{s-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}]: \{0, 1, \ldots, 2^K - 1\} \to \{0, 1\}^K$$

be a bijective mapping, with the convention that the mapping in the case $s = 1$ is denoted by $G[\varnothing]$. Given these mappings, we can define a bijective mapping

$$F: \{0, 1, \ldots, 2^{Kh} - 1\} \to \{0, 1, \ldots, 2^h - 1\}^K \tag{3}$$

as follows. Suppose that n is an integer satisfying $0 \leqslant n < 2^{Kh}$. Write

$$n = \tau_h 2^{K(h-1)} + \tau_{h-1} 2^{K(h-2)} + \ldots + \tau_1, \tag{4}$$

where $\tau_1, \ldots, \tau_h \in \{0, 1, \ldots, 2^K - 1\}$. We now let $\mathbf{a}_1, \ldots, \mathbf{a}_h \in \{0, 1\}^K$ be the solution of the following system of equations:

$$\left.\begin{aligned}
&G[\varnothing](\tau_1) = \mathbf{a}_1,\\
&G[\tau_1; \mathbf{a}_1](\tau_2) = \mathbf{a}_2,\\
&G[\tau_1, \tau_2; \mathbf{a}_1, \mathbf{a}_2](\tau_3) = \mathbf{a}_3,\\
&\quad\vdots\\
&G[\tau_1, \ldots, \tau_{s-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}](\tau_s) = \mathbf{a}_s,\\
&\quad\vdots\\
&G[\tau_1, \ldots, \tau_{h-2}; \mathbf{a}_1, \ldots, \mathbf{a}_{h-2}](\tau_{h-1}) = \mathbf{a}_{h-1},\\
&G[\tau_1, \ldots, \tau_{h-1}; \mathbf{a}_1, \ldots, \mathbf{a}_{h-1}](\tau_h) = \mathbf{a}_h.
\end{aligned}\right\} \tag{5}$$

Suppose now that for each integer $t = 1, \ldots, h$,

$$\mathbf{a}_t = (a_{t,1}, \ldots, a_{t,K}) \in \{0, 1\}^K. \tag{6}$$

We now write

$$F_j(n) = a_{1,j} 2^{h-1} + a_{2,j} 2^{h-2} + \ldots + a_{h,j} \tag{7}$$

and let

$$F(n) = (F_1(n), \ldots, F_k(n)). \tag{8}$$

We next partition U^K into a sequence of 2^{Kh} smaller cubes

$$S(n) = I(2, h, F_1(n)) \times \ldots \times I(2, h, F_k(n)), \tag{9}$$

where, for every $j = 1, \ldots, K$ and every $n = 0, 1, \ldots, 2^{Kh} - 1$, the interval $I(2, h, F_j(n))$ is defined by (2) and (4)–(7). We further extend the range of

definition of $S(n)$ over the set $\mathbb{Z}$ by periodicity so as to ensure that

$$S(n+2^{Kh}) = S(n) \tag{10}$$

for every integer n.

LEMMA 1. *Suppose that s is an integer satisfying $0 \leqslant s \leqslant h$. Then for every integer n_0, the set*

$$\bigcup_{\substack{0 \leqslant n < 2^{Kh} \\ n \equiv n_0 \pmod{2^{Ks}}}} S(n) \tag{11}$$

is a cube of the form

$$C(s, \mathbf{c}) = I(2, s, c_1) \times \ldots \times I(2, s, c_K) \subset U^K, \tag{12}$$

where $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$. On the other hand, every cube of the form (12), *where $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$, is a union of the form* (11) *for some integer n_0.*

Proof. Note that the condition $n \equiv n_0 \pmod{2^{Ks}}$ determines precisely the values of $\tau_1, \ldots, \tau_s$ in (4). We can therefore solve the system of equations

$$\left.\begin{aligned} &G[\varnothing](\tau_1) = \mathbf{a}_1, \\ &G[\tau_1 ; \mathbf{a}_1](\tau_2) = \mathbf{a}_2, \\ &\quad\vdots \\ &G[\tau_1, \ldots, \tau_{s-1} ; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}](\tau_s) = \mathbf{a}_s, \end{aligned}\right\} \tag{13}$$

for $\mathbf{a}_1, \ldots, \mathbf{a}_s$. On the other hand, $\tau_{s+1}, \ldots, \tau_h$ in (4) can take all possible values. It follows from

$$\left.\begin{aligned} &G[\tau_1, \ldots, \tau_s ; \mathbf{a}_1, \ldots, \mathbf{a}_s](\tau_{s+1}) = \mathbf{a}_{s+1}, \\ &\quad\vdots \\ &G[\tau_1, \ldots, \tau_{h-1} ; \mathbf{a}_1, \ldots, \mathbf{a}_{h-1}](\tau_h) = \mathbf{a}_h \end{aligned}\right\} \tag{14}$$

that $\mathbf{a}_{s+1}, \ldots, \mathbf{a}_h$ can take all possible values. The first assertion follows. To prove the second assertion, simply note that $\tau_1, \ldots, \tau_s$ are determined uniquely with given $\mathbf{a}_1, \ldots, \mathbf{a}_s$ by (13), and that if $\mathbf{a}_{s+1}, \ldots, \mathbf{a}_h$ take all possible values, then $\tau_{s+1}, \ldots, \tau_h$ take all possible values in view of (14).

LEMMA 2. *Suppose that s is an integer satisfying $0 \leqslant s \leqslant h$, and that q is an odd natural number. Then for every integer n_0, the set*

$$\bigcup_{\substack{0 \leqslant n < 2^{Kh}q \\ n \equiv n_0 \pmod{2^{Ks}q}}} S(n)$$

is a cube of the form (12), *where $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$.*

Proof. For every n satisfying $0 \leqslant n < 2^{Kh}q$, let $\bar{n}$ satisfy $\bar{n} \equiv n \pmod{2^{Kh}}$ and $0 \leqslant \bar{n} < 2^{Kh}$. Suppose now that $0 \leqslant n_1 < n_2 < 2^{Kh}q$ and $n_1 \equiv n_2 \equiv n_0 \pmod{2^{Ks}q}$. Then $\bar{n}_1 \neq \bar{n}_2$, for otherwise $n_1 \equiv n_2 \pmod{2^{Kh}}$, so that $n_1 \equiv n_2 \pmod{2^{Kh}q}$, a contradiction. On the other hand, if $n \equiv n_0 \pmod{2^{Ks}q}$, then $\bar{n} \equiv n_0 \pmod{2^{Ks}}$.

Hence

$$\{\bar{n}:\ 0 \leqslant n < 2^{Kh}q \text{ and } n \equiv n_0 \pmod{2^{Ks}q}\} = \{0 \leqslant m < 2^{Kh}:\ m \equiv n_0 \pmod{2^{Ks}}\},$$

since they have the same number of elements. The lemma now follows from Lemma 1 on noting that $S(n) = S(\bar{n})$.

For every $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^h - 1\}^K$, let $\mathbf{q}(\mathbf{c})$ be a point in the cube

$$C(h\,;\mathbf{c}) = I(2, h, c_1) \times \ldots \times I(2, h, c_K) \subset U^K.$$

Using F, we can define a permutation $\mathbf{q}_n$ $(0 \leqslant n < 2^{Kh})$ of the $\mathbf{q}(\mathbf{c})$ as follows. For $n = 0, 1, \ldots, 2^{Kh} - 1$, let

$$\mathbf{q}_n = \mathbf{q}(F(n)) = \mathbf{q}(F_1(n), \ldots, F_K(n)).$$

Clearly $\mathbf{q}_n \in S(n)$ for every $n = 0, 1, \ldots, 2^{Kh} - 1$. Again, we extend the range of definition of $\mathbf{q}_n$ over the set $\mathbb{Z}$ by periodicity with period 2^{Kh} so as to ensure that $\mathbf{q}_n \in S(n)$ for every integer n. Then it follows from Lemma 1 that

LEMMA 3. *Suppose that s and H are integers satisfying $0 \leqslant s \leqslant h$ and $H \geqslant 0$. Then every cube of the form* (12), *where $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$, contains exactly one element of the set $\{\mathbf{q}_n:\ H2^{Ks} \leqslant n < (H+1)2^{Ks}\}$.*

Proof. We may assume, without loss of generality, that $H < 2^{K(h-s)}$. Then the restriction $H2^{Ks} \leqslant n < (H+1)2^{Ks}$ determines precisely the values of $\tau_{s+1}, \ldots, \tau_h$ in (4) with no restriction on $\tau_1, \ldots, \tau_s$. On the other hand, the restriction $\mathbf{q}_n \in C(s\,;\mathbf{c})$ for a given $\mathbf{c}$ determines precisely the values of $\mathbf{a}_1, \ldots, \mathbf{a}_s$ with no restriction on $\mathbf{a}_{s+1}, \ldots, \mathbf{a}_h$. The system of equations

$$\left.\begin{aligned} &G[\varnothing](\tau_1) = \mathbf{a}_1, \\ &G[\tau_1\,;\mathbf{a}_1](\tau_2) = \mathbf{a}_2, \\ &\quad\vdots \\ &G[\tau_1, \ldots, \tau_{s-1}\,;\mathbf{a}_1, \ldots, \mathbf{a}_{s-1}](\tau_s) = \mathbf{a}_s \end{aligned}\right\}$$

now determines precisely the values of $\tau_1, \ldots, \tau_s$. Hence n is uniquely determined.

We denote this element obtained by Lemma 3 by $\mathbf{q}(s\,;\mathbf{c}\,;H)$. In other words, for integers $s, c_1, \ldots, c_K, H$ satisfying the hypotheses of Lemma 3,

$$\mathbf{q}(s\,;\mathbf{c}\,;H) = \{\mathbf{q}_n:\ H2^{Ks} \leqslant n < (H+1)2^{Ks}\} \cap C(s\,;\mathbf{c}).$$

Observe that Lemma 3 is essentially Lemma 1 of Beck and Chen [2], although the construction here is slightly different. We also need Lemma 2 as it is crucial to establish the following key lemma.

LEMMA 4. *Let q be an odd natural number and let n_0 be an integer satisfying $0 \leqslant n_0 < q$. Then for every bijective mapping F of the form* (3) *defined by* (4)–(8), *there exists a corresponding bijective mapping F' of the same type such that $S(n_0 + qn) = S'(n)$ for every $n \in \mathbb{Z}$, where S' is defined in terms of F' in the same way as S is defined in terms of F by* (8) *and* (9).

Proof. By Lemma 2, for every n_1 satisfying $0 \leqslant n_1 < 2^K$, we have that

$$\bigcup_{\substack{0 \leqslant n < 2^{Kh} \\ n \equiv n_1 \pmod{2^K}}} S(n_0 + qn) = \bigcup_{\substack{0 \leqslant m < 2^{Kh} q \\ m \equiv n_0 + qn_1 \pmod{2^K q}}} S(m)$$

is a cube of the form $C(1, \mathbf{c}_1)$, where $\mathbf{c}_1 = (c_{1,1}, \ldots, c_{K,1}) \in \{0, 1\}^K$. Write

$$n = \tau_h 2^{K(h-1)} + \tau_{h-1} 2^{K(h-2)} + \ldots + \tau_1.$$

If $n \equiv n_1 \pmod{2^K}$, then τ_1 is uniquely determined. As n_1 runs through a complete set of residues modulo 2^K, τ_1 runs through the set $\{0, 1, \ldots, 2^K - 1\}$ while $\mathbf{c}_1$ runs through the set $\{0, 1\}^K$. It follows that writing

$$c_{j,1} 2^{h-1} = b_{1,j} 2^{h-1} \quad \text{and} \quad \mathbf{b}_1 = (b_{1,1}, \ldots, b_{1,K}) \in \{0, 1\}^K,$$

we can establish a bijective mapping between $\{0, 1, \ldots, 2^K - 1\}$ and $\{0, 1\}^K$ represented by $G'[\varnothing](\tau_1) = \mathbf{b}_1$. Suppose now that for every n_s satisfying $0 \leqslant n_s < 2^{Ks}$, the union

$$\bigcup_{\substack{0 \leqslant n < 2^{Kh} \\ n \equiv n_s \pmod{2^{Ks}}}} S(n_0 + qn) \tag{15}$$

is a cube of the form $C(s, \mathbf{c}_s)$, where $\mathbf{c}_s = (c_{1,s}, \ldots, c_{K,s}) \in \{0, 1, \ldots, 2^s - 1\}^K$. Suppose further that, writing

$$c_{j,s} 2^{h-s} = b_{1,j} 2^{h-1} + \ldots + b_{s,j} 2^{h-s}$$

and

$$\mathbf{b}_t = (b_{t,1}, \ldots, b_{t,K}) \in \{0, 1\}^K$$

for every $t = 1, \ldots, s$, we can establish bijective mappings between $\{0, 1, \ldots, 2^K - 1\}$ and $\{0, 1\}^K$ represented by

$$\left.\begin{aligned} &G'[\varnothing](\tau_1) = \mathbf{b}_1, \\ &G'[\tau_1 ; \mathbf{b}_1](\tau_2) = \mathbf{b}_2, \\ &\quad \vdots \\ &G'[\tau_1, \ldots, \tau_{s-1} ; \mathbf{b}_1, \ldots, \mathbf{b}_{s-1}](\tau_s) = \mathbf{b}_s. \end{aligned}\right\}$$

We now consider a fixed n_s, so that $\tau_1, \ldots, \tau_s, \mathbf{b}_1, \ldots, \mathbf{b}_s$ are uniquely determined. Consider the residue class $n \equiv n_s \pmod{2^{Ks}}$. This is the union of 2^K residue classes modulo $2^{K(s+1)}$. We denote them by

$$n \equiv \tau_{s+1} 2^{Ks} + n_s \pmod{2^{K(s+1)}},$$

where $\tau_{s+1} \in \{0, 1, \ldots, 2^K - 1\}$. By Lemma 2, for each such τ_{s+1}, the union

$$\bigcup_{\substack{0 \leqslant n < 2^{Kh} \\ n \equiv \tau_{s+1} 2^{Ks} + n_s \pmod{2^{K(s+1)}}}} S(n_0 + qn)$$

is a cube of the form $C(s+1, \mathbf{c}_{s+1}) \subset C(s, \mathbf{c}_s)$, where

$$\mathbf{c}_{s+1} = (c_{1,s+1}, \ldots, c_{K,s+1}) \in \{0, 1, \ldots, 2^{s+1} - 1\}^K.$$

It follows that

$$c_{j,s+1} 2^{h-s-1} = b_{1,j} 2^{h-1} + \ldots + b_{s,j} 2^{h-s} + b_{s+1,j} 2^{h-s-1},$$

where $b_{1,j}, \ldots, b_{s,j}$ are fixed. As τ_{s+1} runs through the set $\{0, 1, \ldots, 2^K - 1\}$,

$$\mathbf{b}_{s+1} = (b_{s+1,1}, \ldots, b_{s+1,K})$$

runs through the set $\{0, 1\}^K$. We can therefore establish a bijective mapping between $\{0, 1, \ldots, 2^K - 1\}$ and $\{0, 1\}^K$ represented by

$$G'[\tau_1, \ldots, \tau_s ; \mathbf{b}_1, \ldots, \mathbf{b}_s](\tau_{s+1}) = \mathbf{b}_{s+1}.$$

By induction, it follows that for every n_h satisfying $0 \leqslant n_h < 2^{Kh}$, $S(n_0 + qn)$ is a cube of the form $C(h, \mathbf{c}_h)$, where $\mathbf{c}_h = (c_{1,h}, \ldots, c_{K,h}) \in \{0, 1, \ldots, 2^h - 1\}^K$; and that writing

$$c_{j,h} = b_{1,j}2^{h-1} + \ldots + b_{h,j}$$

and

$$\mathbf{b}_t = (b_{t,1}, \ldots, b_{t,K}) \in \{0, 1\}^K$$

for every $t = 1, \ldots, h$, we can establish a system of bijective mappings between $\{0, 1, \ldots, 2^K - 1\}$ and $\{0, 1\}^K$ represented by

$$\left.\begin{aligned} &G'[\varnothing](\tau_1) = \mathbf{b}_1, \\ &G'[\tau_1 ; \mathbf{b}_1](\tau_2) = \mathbf{b}_2, \\ &\quad\vdots \\ &G'[\tau_1, \ldots, \tau_{h-1} ; \mathbf{b}_1, \ldots, \mathbf{b}_{h-1}](\tau_h) = \mathbf{b}_h. \end{aligned}\right\}$$

The lemma now follows easily.

5. *Some probabilistic lemmas*

As in [2], we now use some elementary concepts and facts from probability theory (see, for example, Chung [6]), and define a 'randomization' of the deterministic points $\mathbf{q}(\mathbf{c}) = \mathbf{q}(c_1, \ldots, c_K)$, mappings $G[\tau_1, \ldots, \tau_{s-1} ; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}]$ and F, and the sequence $\mathbf{q}_n$ as follows.

(A) For $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^h - 1\}^K$, let $\tilde{\mathbf{q}}(\mathbf{c})$ be a random point uniformly distributed in the cube $C(h ; \mathbf{c})$. More precisely,

$$\text{Prob}(\tilde{\mathbf{q}}(\mathbf{c}) \in \mathscr{S}) = \mu_K(C(h ; \mathbf{c}) \cap \mathscr{S})/\mu_K(C(h; \mathbf{c}))$$

for all Borel sets $\mathscr{S} \subset \mathbb{R}^K$.

(B) For every integer s satisfying $1 \leqslant s \leqslant h$, integers

$$\tau_1, \ldots, \tau_{s-1} \in \{0, 1, \ldots, 2^K - 1\}$$

and vectors $\mathbf{a}_1, \ldots, \mathbf{a}_{s-1} \in \{0, 1\}^K$, let $\tilde{G}[\tau_1, \ldots, \tau_{s-1} ; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}]$ be a uniformly distributed random bijective mapping from $\{0, 1, \ldots, 2^K - 1\}$ to $\{0, 1\}^K$. More precisely, if π: $\{0, 1, \ldots, 2^K - 1\} \to \{0, 1\}^K$ is one of the $(2^K)!$ different (deterministic) bijective mappings, then

$$\text{Prob}(\tilde{G}[\tau_1, \ldots, \tau_{s-1} ; \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}] = \pi) = 1/(2^K)!.$$

(C) Let $\tilde{F}$ be the random bijective mapping from $\{0, 1, \ldots, 2^{Kh} - 1\}$ to $\{0, 1, \ldots, 2^h - 1\}^K$ defined by (4), ($\tilde{5}$) and (6)–(8), where ($\tilde{5}$) denotes that in the system (5) of equations, we replace each deterministic mapping by its corresponding random mapping.

(D) Let $\tilde{\mathbf{q}}_n$ $(0 \leqslant n < 2^{Kh})$ denote the random sequence defined by $\tilde{F}$; *i.e.*, for $n = 0, 1, \ldots, 2^{Kh} - 1$,

$$\tilde{\mathbf{q}}_n = \mathbf{q}(\tilde{F}(n));$$

again, we extend $\tilde{\mathbf{q}}_n$ over the set $\mathbb{Z}$ by periodicity with period 2^{Kh}.

(E) Let $\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H)$ denote the randomization of $\mathbf{q}(s\,;\mathbf{c}\,;H)$; *i.e.*, for integers $s, c_1, \ldots, c_K, H$ satisfying the hypotheses of Lemma 3,

$$\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H) = \{\tilde{\mathbf{q}}_n\colon\ H2^{Ks} \leqslant n < (H+1)2^{Ks}\} \cap C(s\,;\mathbf{c}). \tag{16}$$

(F) Finally, we may assume that the random variables

$$\tilde{\mathbf{q}}(\mathbf{c}) \quad (\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^h - 1\}^K)$$

and

$$\tilde{G}[\tau_1, \ldots, \tau_{s-1}\,;\mathbf{a}_1, \ldots, \mathbf{a}_{s-1}] \quad (1 \leqslant s \leqslant h \text{ and } \tau_1, \ldots, \tau_{s-1} \in \{0, 1, \ldots, 2^K - 1\} \text{ and } \mathbf{a}_1, \ldots, \mathbf{a}_{s-1} \in \{0, 1\}^K)$$

are independent of each other. In fact, the existence of such a set of random variables follows immediately from the Kolmogorov extension theorem in probability theory.

Let $(\Omega, \mathcal{F}, \text{Prob})$ denote the underlying probability measure space.

As in [2], we have

LEMMA 5. *Suppose that s and H are integers satisfying $0 \leqslant s \leqslant h$ and $H \geqslant 0$. Then for every $\mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K$, the random point $\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H)$ is uniformly distributed in the cube $C(s\,;\mathbf{c})$.*

Proof. Suppose that for $j = 1, \ldots, K$,

$$c_j = a_{1,j}2^{s-1} + a_{2,j}2^{s-2} + \ldots + a_{s,j}.$$

For $t = 1, \ldots, s$, let $\mathbf{a}_t = (a_{t,1}, \ldots, a_{t,K})$. Since the random mapping $\tilde{G}[\varnothing]$ is uniformly distributed, it follows that the (random) solution $\tilde{\tau}_1$ of the equation $\tilde{G}[\varnothing](\tilde{\tau}_1) = \mathbf{a}_1$ has the property that for any $\delta \in \{0, 1, \ldots, 2^K - 1\}$,

$$\text{Prob}(\tilde{\tau}_1 = \delta) = 2^{-K}.$$

Now let $\tilde{\tau}_1 = \tau_1$ (*i.e.* fix the value of this random variable), and consider the (random) equation

$$\tilde{G}[\tau_1\,;\mathbf{a}_1](\tilde{\tau}_2) = \mathbf{a}_2.$$

Since $\tilde{G}[\tau_1\,;\mathbf{a}_1]$ is also uniformly distributed, we have, for any $\delta = \{0, 1, \ldots, 2^K - 1\}$, that

$$\text{Prob}(\tilde{\tau}_2 = \delta \mid \tau_1 = \tau) = 2^{-K}.$$

In other words, the random variables $\tilde{\tau}_1$ and $\tilde{\tau}_2$ are independent of each other. Repeating this argument, we conclude that $\tilde{\tau}_1, \ldots, \tilde{\tau}_s$, obtained from

$$\left.\begin{aligned} &\tilde{G}[\varnothing](\tilde{\tau}_1) = \mathbf{a}_1, \\ &\tilde{G}[\tau_1\,;\mathbf{a}_1](\tilde{\tau}_2) = \mathbf{a}_2, \\ &\quad\vdots \\ &\tilde{G}[\tau_1, \ldots, \tau_{s-1}\,;\mathbf{a}_1, \ldots, \mathbf{a}_{s-1}](\tilde{\tau}_s) = \mathbf{a}_s, \end{aligned}\right\}$$

are independent random variables with common distribution function

$$\text{Prob}(\tilde{\tau}_t = \delta) = 2^{-K}$$

for every $t = 1, \ldots, s$ and $\delta \in \{0, 1, \ldots, 2^K - 1\}$. Let

$$\tilde{n}_0 = \tilde{\tau}_s 2^{K(s-1)} + \tilde{\tau}_{s-1} 2^{K(s-2)} + \ldots + \tilde{\tau}_1.$$

Then $\tilde{n}_0$ is uniformly distributed in the set $\{0, 1, \ldots, 2^{Ks} - 1\}$. Write

$$\tilde{n} = \tau_h 2^{K(h-1)} + \ldots + \tau_{s+1} 2^{Ks} + \tilde{n}_0,$$

where

$$H 2^{Ks} = \tau_h 2^{K(h-1)} + \ldots + \tau_{s+1} 2^{Ks}$$

(note that, as in Lemma 3, we may assume, without loss of generality, that $H < 2^{K(h-s)}$). Then $\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H) = \tilde{\mathbf{q}}_{\tilde{n}}$. Suppose now that $H2^{Ks} \leqslant n < (H+1)2^{Ks}$. Then

$$\text{Prob}(\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H) = \tilde{\mathbf{q}}_n) = \text{Prob}(\tilde{n} = n) = 2^{-Ks}.$$

Since $\tilde{\mathbf{q}}_n$ is uniformly distributed in $S(n)$ for every n satisfying $H2^{Ks} \leqslant n < (H+1)2^{Ks}$, the result follows from the independence of $\tilde{n}$ and $\tilde{\mathbf{q}}_n$.

Let $\mathscr{S}$ be a fixed compact and convex set in U^K. For integers s and H satisfying $0 \leqslant s \leqslant h$ and $H \geqslant 0$, consider the random set

$$\tilde{\mathscr{P}}(s, H) = \{\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H):\ \mathbf{c} = (c_1, \ldots, c_K) \in \{0, 1, \ldots, 2^s - 1\}^K\}, \tag{17}$$

and write

$$Z_K[\tilde{\mathscr{P}}(s, H)\,;\mathscr{S}] = \#(\tilde{\mathscr{P}}(s, H) \cap \mathscr{S})$$

and

$$\tilde{D}_K(s, H) = Z_K[\tilde{\mathscr{P}}(s, H)\,;\mathscr{S}] - 2^{Ks}\mu_K(\mathscr{S}). \tag{18}$$

Note that $\tilde{D}_K(s, H)$ depends on $\mathscr{S}$. Let

$$T(s, H) = \{\mathbf{c} \in \{0, 1, \ldots, 2^s - 1\}^K:\ C(s\,;\mathbf{c}) \cap \mathscr{S} \neq \varnothing \text{ and } C(s\,;\mathbf{c}) \setminus \mathscr{S} \neq \varnothing\}. \tag{19}$$

It is easy to see that

$$\#T(s, H) \leqslant 2K2^{(K-1)s}. \tag{20}$$

Since every cube $C(s\,;\mathbf{c})$ contains exactly one element (namely $\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H)$) of the (random) set $\tilde{\mathscr{P}}(s, H)$, we have

$$\tilde{D}_K(s, H) = \sum_{\substack{\mathbf{c} \in T(s, H) \\ \tilde{\mathbf{q}}(s;\mathbf{c};H) \in \mathscr{S}}} 1 - 2^{Ks} \sum_{\mathbf{c} \in T(s, H)} \mu_K(C(s\,;\mathbf{c}) \cap \mathscr{S}).$$

For every $\mathbf{c} \in T(s, H)$, let

$$\xi(s\,;\mathbf{c}\,;H) = \begin{cases} 1 & (\tilde{\mathbf{q}}(s\,;\mathbf{c}\,;H) \in \mathscr{S}), \\ 0 & (\text{otherwise}). \end{cases}$$

By Lemma 5, we have, writing $\mathbb{E}$ for 'expected value',

$$\mathbb{E}\xi(s\,;\mathbf{c}\,;H) = \frac{\mu_K(C(s\,;\mathbf{c}) \cap \mathscr{S})}{\mu_K(C(s\,;\mathbf{c}))} = 2^{Ks}\mu_K(C(s\,;\mathbf{c}) \cap \mathscr{S}), \tag{21}$$

so that writing

$$\eta(s\,;\mathbf{c}\,;H) = \xi(s\,;\mathbf{c}\,;H) - \mathbb{E}\xi(s\,;\mathbf{c}\,;H),$$

we have

$$\tilde{D}_K(s, H) = \sum_{\mathbf{c} \in T(s,H)} \eta(s\,;\mathbf{c}\,;H). \tag{22}$$

Note that $\mathbb{E}\eta = 0$ and $|\eta| \leqslant 1$.

We need the following analogue of Lemma 3 of [2].

LEMMA 6. *Suppose that* s', $s'' \in \{0, 1, \ldots, h\}$, H' *and* H'' *are non-negative integers,* $\mathbf{c}' \in \{0, 1, \ldots, 2^{s'}-1\}^K$ *and* $\mathbf{c}'' \in \{0, 1, \ldots, 2^{s''}-1\}^K$. *Suppose further that either*

(i) $s' = s''$ *and* $\mathbf{c}' \neq \mathbf{c}''$; *or*

(ii) $s' > s''$.

Then

$$\mathbb{E}(\eta(s'; \mathbf{c}'; H')\eta(s''; \mathbf{c}''; H'')) \leq \frac{\mu_K(C(s'; \mathbf{c}') \cap C(s''; \mathbf{c}''))}{\mu_K(C(s''; \mathbf{c}''))}.$$

For convenience of notation, we write

$$C' = C(s'; \mathbf{c}') \quad \text{and} \quad C'' = C(s''; \mathbf{c}''),$$
$$\xi' = \xi(s'; \mathbf{c}'; H') \quad \text{and} \quad \xi'' = \xi(s''; \mathbf{c}''; H''),$$
$$\eta' = \xi' - \mathbb{E}\xi' \quad \text{and} \quad \eta'' = \xi'' - \mathbb{E}\xi''.$$

The proof of Lemma 6 depends on

LEMMA 7. *Let* s', s'', $\mathbf{c}'$, $\mathbf{c}''$ *be defined as in Lemma* 6. *Suppose further that* $\mathbf{c}^* \in \{0, 1, \ldots, 2^h - 1\}^K$ *and* $C(h; \mathbf{c}^*) \subset C'' \setminus C'$. *Consider the event* $\mathcal{A}$ *defined by*

$$\mathcal{A} = \mathcal{A}(s'', \mathbf{c}'', H'', \mathbf{c}^*) \Leftrightarrow \tilde{\mathbf{q}}(s''; \mathbf{c}''; H'') \in C(h; \mathbf{c}^*).$$

Then, writing

$$\xi^* = \xi(h; \mathbf{c}^*; 0) = \begin{cases} 1 & (\tilde{\mathbf{q}}(\mathbf{c}^*) \in \mathcal{S}), \\ 0 & (\text{otherwise}), \end{cases}$$

we have

$$\mathbb{E}(\xi'\xi'' \mid \mathcal{A}) = \mathbb{E}(\xi')\mathbb{E}(\xi^*). \tag{23}$$

Proof of Lemma 6. Let

$$V = \{\mathbf{c} \in \{0, 1, \ldots, 2^h - 1\}^K : C(h; \mathbf{c}) \subset C'' \setminus C'\},$$

and consider the event

$$\mathcal{A}(\mathbf{c}) \Leftrightarrow \tilde{\mathbf{q}}(s''; \mathbf{c}''; H'') \in C(h; \mathbf{c}).$$

Let $\mathcal{C} = \bigcup_{\mathbf{c} \in V} \mathcal{A}(\mathbf{c})$. By (23),

$$\mathbb{E}(\xi'\xi'' \mid \mathcal{C}) = \sum_{\mathbf{c} \in V} \frac{\text{Prob}(\mathcal{A}(\mathbf{c}))}{\text{Prob}(\mathcal{C})} \mathbb{E}(\xi')\mathbb{E}(\xi(\mathbf{c})), \tag{24}$$

where

$$\xi(\mathbf{c}) = \xi(h; \mathbf{c}; 0) = \begin{cases} 1 & (\tilde{\mathbf{q}}(\mathbf{c}) \in \mathcal{S}), \\ 0 & (\text{otherwise}). \end{cases}$$

By Lemma 5, for every $\mathbf{c} \in V$, we clearly have

$$\text{Prob}(\mathcal{A}(\mathbf{c})) = \text{Prob}(\tilde{\mathbf{q}}(s''; \mathbf{c}''; H'') \in C(h; \mathbf{c})) = 2^{-K(h-s'')}. \tag{25}$$

On the other hand,

$$\mathbb{E}(\xi') = 2^{Ks'} \mu_K(C' \cap \mathcal{S}) \tag{26}$$

and

$$\mathbb{E}(\xi'') = 2^{Ks''} \mu_K(C'' \cap \mathcal{S}). \tag{27}$$

Furthermore,

$$\mathbb{E}(\xi(\mathbf{c})) = \frac{\mu_K(C(h\,;\mathbf{c}) \cap \mathcal{S})}{\mu_K(C(h\,;\mathbf{c}))} = 2^{Kh}\mu_K(C(h\,;\mathbf{c}) \cap \mathcal{S}), \tag{28}$$

and

$$\mathrm{Prob}(\mathscr{C}) = \mu_K(C'' \setminus C')/\mu_K(C''). \tag{29}$$

Combining (24)–(26) and (28), we have

$$\begin{aligned}\mathbb{E}(\xi'\xi'' \mid \mathscr{C}) &= \frac{2^{K(s'+s'')}}{\mathrm{Prob}(\mathscr{C})} \sum_{\mathbf{c} \in V} \mu_K(C' \cap \mathcal{S})\mu_K(C(h\,;\mathbf{c}) \cap \mathcal{S}) \\ &= \frac{2^{K(s'+s'')}}{\mathrm{Prob}(\mathscr{C})} \mu_K(C' \cap \mathcal{S})\mu_K((C'' \setminus C') \cap \mathcal{S}).\end{aligned} \tag{30}$$

Clearly

$$\mathbb{E}(\eta'\eta'') = \mathbb{E}(\xi'\xi'') - \mathbb{E}(\xi')\mathbb{E}(\xi'') \tag{31}$$

and

$$\mathbb{E}(\xi'\xi'') = \mathrm{Prob}(\mathscr{C})\mathbb{E}(\xi'\xi'' \mid \mathscr{C}) + (1 - \mathrm{Prob}(\mathscr{C}))\mathbb{E}(\xi'\xi'' \mid \Omega \setminus \mathscr{C}). \tag{32}$$

By (26) and (27),

$$\mathbb{E}(\xi')\mathbb{E}(\xi'') = 2^{K(s'+s'')}\mu_K(C' \cap \mathcal{S})\mu_K(C'' \cap \mathcal{S}). \tag{33}$$

On combining (30) and (33), we have

$$\begin{aligned}&\mathbb{E}(\xi')\mathbb{E}(\xi'') - \mathrm{Prob}(\mathscr{C})\mathbb{E}(\xi'\xi'' \mid \mathscr{C}) \\ &\qquad = \frac{\mu_K(C' \cap \mathcal{S})\mu_K(C'' \cap \mathcal{S}) - \mu_K(C' \cap \mathcal{S})\mu_K((C'' \setminus C') \cap \mathcal{S})}{\mu_K(C')\mu_K(C'')} \\ &\qquad = \frac{\mu_K(C' \cap \mathcal{S})\mu_K((C' \cap C'') \cap \mathcal{S})}{\mu_K(C')\mu_K(C'')}.\end{aligned} \tag{34}$$

It follows from (31), (32) and (34) that

$$\mathbb{E}(\eta'\eta'') = (1 - \mathrm{Prob}(\mathscr{C}))\mathbb{E}(\xi'\xi'' \mid \Omega \setminus \mathscr{C}) - \frac{\mu_K(C' \cap \mathcal{S})\mu_K((C' \cap C'') \cap \mathcal{S})}{\mu_K(C')\mu_K(C'')}. \tag{35}$$

Since $0 \leqslant \xi',\ \xi'' \leqslant 1$, we have

$$0 \leqslant \mathbb{E}(\xi'\xi'' \mid \Omega \setminus \mathscr{C}) \leqslant 1. \tag{36}$$

Furthermore,

$$0 \leqslant \frac{\mu_K(C' \cap \mathcal{S})\mu_K((C' \cap C'') \cap \mathcal{S})}{\mu_K(C')\mu_K(C'')} \leqslant \frac{\mu_K(C' \cap C'')}{\mu_K(C'')}. \tag{37}$$

On combining (29) and (35)–(37), we conclude that

$$-\frac{\mu_K(C' \cap C'')}{\mu_K(C'')} \leqslant \mathbb{E}(\eta'\eta'') \leqslant 1 - \mathrm{Prob}(\mathscr{C}) = \frac{\mu_K(C' \cap C'')}{\mu_K(C'')},$$

and Lemma 6 follows.

We conclude this section by proving Lemma 7. Let

$$\mathbf{c}^* = (c_1^*, \ldots, c_K^*) \in \{0, 1, \ldots, 2^h - 1\}^K,$$

where for every $j = 1, \ldots, K$,

$$c^* = c_{1,j}^* 2^{h-1} + c_{2,j}^* 2^{h-2} + \ldots + c_{h,j}^*,$$

where $c^*_{1,j}, \ldots, c^*_{h,j} \in \{0, 1\}$. For every $s = 1, \ldots, h$, let $\mathbf{c}^*_s = (c^*_{s,1}, \ldots, c^*_{s,K})$. Furthermore, let

$$H''2^{Ks''} = \tau_h 2^{K(h-1)} + \ldots + \tau_{s''+1}2^{Ks''},$$

where $\tau_{s''+1}, \ldots, \tau_h \in \{0, 1, \ldots, 2^K - 1\}$. Then every natural number n in the range $H''2^{Ks''} \leq n < (H''+1)2^{Ks''}$ can be written in the form

$$n = H''2^{Ks''} + \tau_{s''}2^{K(s''-1)} + \ldots + \tau_1,$$

where $\tau_1, \ldots, \tau_{s''} \in \{0, 1, \ldots, 2^K - 1\}$. Event $\mathscr{A}$ is equivalent to the fulfillment of the system

$$\left.\begin{aligned} &\bar{G}[\tau_1, \ldots, \tau_{s''}; \mathbf{c}^*_1, \ldots, \mathbf{c}^*_{s''}](\tau_{s''+1}) = \mathbf{c}^*_{s''+1}, \\ &\quad\vdots \\ &\bar{G}[\tau_1, \ldots, \tau_{h-1}; \mathbf{c}^*_1, \ldots, \mathbf{c}^*_{h-1}](\tau_h) = \mathbf{c}^*_h, \end{aligned}\right\} \tag{38}$$

of random equations for some $\tau_1, \ldots, \tau_{s''} \in \{0, 1, \ldots, 2^K - 1\}$. Now let $\mathbf{c}' = (c'_1, \ldots, c'_K)$, where for every $j = 1, \ldots, K$,

$$c'_j 2^{h-s'} = c'_{1,j}2^{h-1} + c'_{2,j}2^{h-2} + \ldots + c'_{s',j}2^{h-s'},$$

where $c'_{1,j}, \ldots, c'_{s',j} \in \{0, 1\}$. For every $t = 1, \ldots, s'$, let $\mathbf{c}'_t = (c'_{t,1}, \ldots, c'_{t,K})$. Furthermore, let

$$H'2^{Ks'} = \lambda_h 2^{K(h-1)} + \ldots + \lambda_{s'+1}2^{Ks'},$$

where $\lambda_{s'+1}, \ldots, \lambda_h \in \{0, 1, \ldots, 2^K - 1\}$. Then the random variable $\tilde{\mathbf{q}}(s'; \mathbf{c}'; H')$ depends only on the following random variables: the random mappings

$$\left.\begin{aligned} &\bar{G}[\lambda_1, \ldots, \lambda_{s'}; \mathbf{c}'_1, \ldots, \mathbf{c}'_{s'}], \\ &\bar{G}[\lambda_1, \ldots, \lambda_{s'+1}; \mathbf{c}'_1, \ldots, \mathbf{c}'_{s'}; \mathbf{d}_{s'+1}], \\ &\quad\vdots \\ &\bar{G}[\lambda_1, \ldots, \lambda_{h-1}; \mathbf{c}'_1, \ldots, \mathbf{c}'_{s'}, \mathbf{d}_{s'+1}, \ldots, \mathbf{d}_{h-1}], \end{aligned}\right\} \tag{39a}$$

where $\lambda_1, \ldots, \lambda_{s'} \in \{0, 1, \ldots, 2^K - 1\}$ and $\mathbf{d}_{s'+1}, \ldots, \mathbf{d}_{h-1} \in \{0, 1\}^K$; and the random points

$$\{\tilde{\mathbf{q}}(\mathbf{c}):\ C(h; \mathbf{c}) \subset C(s'; \mathbf{c}')\}. \tag{39b}$$

Consider now the following three sets of random variables;

$$\left.\begin{aligned} &\{\tilde{\mathbf{q}}(\mathbf{c}^*)\}, \\ &\{\text{random mappings occurring in (38)}\}, \\ &\{\text{random mappings and points occurring in (39)}\}. \end{aligned}\right\}$$

Note that these three sets are pairwise disjoint, since the assumption $C(h; \mathbf{c}^*) \subset C''\backslash C'$ yields $(\mathbf{c}'_1, \ldots, \mathbf{c}'_{s''}) \neq (\mathbf{c}^*_1, \ldots, \mathbf{c}^*_{s''})$. Lemma 7 follows immediately from

LEMMA 8. *Let* $(\Omega, \mathscr{F}, \text{Prob})$ *be a probability measure space. Let* $\mathscr{A} \in \mathscr{F}$, *and let* ξ', ξ'' *and* ξ^* *be random variables on this space. Suppose that*

$$\mathscr{A} \Leftrightarrow \xi'' = \xi^*.$$

Furthermore, suppose that ξ', ξ^* and $\chi_{\mathscr{A}}$ (characteristic function of the event $\mathscr{A}$) are independent. Then

$$\mathbb{E}(\xi'\xi'' \mid \mathscr{A}) = \mathbb{E}(\xi')\mathbb{E}(\xi^*). \tag{40}$$

Proof. By definition,

$$\begin{aligned}\mathbb{E}(\xi'\xi'' \mid \mathscr{A}) &= \frac{1}{\text{Prob}(\mathscr{A})}\int_{\mathscr{A}} \xi'(\omega)\xi''(\omega)\, d\,\text{Prob}(\omega)\\ &= \frac{1}{\text{Prob}(\mathscr{A})}\int_{\mathscr{A}} \xi'(\omega)\xi^*(\omega)\, d\,\text{Prob}(\omega)\\ &= \frac{1}{\text{Prob}(\mathscr{A})}\int_{\Omega} \xi'(\omega)\xi^*(\omega)\chi_{\mathscr{A}}(\omega)\, d\,\text{Prob}(\omega).\end{aligned} \tag{41}$$

By the independence of ξ', ξ^* and $\chi_{\mathscr{A}}$, we have

$$\int_{\Omega} \xi'(\omega)\xi^*(\omega)\chi_{\mathscr{A}}(\omega)\, d\,\text{Prob}(\omega) = \mathbb{E}(\xi')\mathbb{E}(\xi^*)\mathbb{E}(\chi_{\mathscr{A}}) = \mathbb{E}(\xi')\mathbb{E}(\xi^*)\text{Prob}(\mathscr{A}). \tag{42}$$

Equation (40) follows immediately on combining (41) and (42).

6. *An intermediate result*

In this section, we aim to prove an intermediate result (Lemma 10 below) for application later. The proof of this intermediate result depends on the following lemma. For every natural number M, let

$$\bar{\mathscr{Q}}_M = \{\tilde{\mathbf{q}}_0, \tilde{\mathbf{q}}_1, \ldots, \tilde{\mathbf{q}}_{M-1}\} \tag{43}$$

and, for every compact and convex set $\mathscr{S} \subset U^K$, let

$$Z_K[\bar{\mathscr{Q}}_M\,;\,\mathscr{S}] = \#(\bar{\mathscr{Q}}_M \cap \mathscr{S}),$$

and write

$$D_K[\bar{\mathscr{Q}}_M\,;\,\mathscr{S}] = Z_K[\bar{\mathscr{Q}}_M\,;\,\mathscr{S}] - M\mu_K(\mathscr{S}). \tag{44}$$

LEMMA 9. *For every natural number M satisfying $1 \leqslant M \leqslant 2^{Kh}$, we have*

$$\mathbb{E}(D_K[\bar{\mathscr{Q}}_M\,;\,\mathscr{S}])^2 \leqslant K2^{4K}M^{1-1/K}.$$

Proof. Write

$$M - 1 = \tau_h 2^{K(h-1)} + \tau_{h-1}2^{K(h-2)} + \ldots + \tau_1,$$

where $\tau_1, \ldots, \tau_h \in \{0, 1, \ldots, 2^K - 1\}$. Suppose that $\tau_{k+1} = \ldots = \tau_h = 0$ and $\tau_k \neq 0$. Then

$$\{\tilde{\mathbf{q}}_0, \tilde{\mathbf{q}}_1, \ldots, \tilde{\mathbf{q}}_{M-1}\} = \bigcup_{s=1}^{k}\bigcup_{m_s=0}^{\tau_s-1}\{\tilde{\mathbf{q}}_n\colon\ M_s + m_s 2^{K(s-1)} \leqslant n < M_s + (m_s+1)2^{K(s-1)}\}, \tag{45}$$

where, for $1 \leqslant s \leqslant k$,

$$\begin{aligned}M_s &= \tau_h 2^{K(h-1)} + \tau_{h-1}2^{K(h-2)} + \ldots + \tau_{s+1}2^{Ks}\\ &= \tau_k 2^{K(k-1)} + \tau_{k-1}2^{K(k-2)} + \ldots + \tau_{s+1}2^{Ks}.\end{aligned} \tag{46}$$

Note that

$$M \geqslant 2^{K(k-1)}. \tag{47}$$

It now follows from (16), (17), (45) and (46) that

$$\{\tilde{\mathbf{q}}_0, \tilde{\mathbf{q}}_1, \ldots, \tilde{\mathbf{q}}_{M-1}\} = \bigcup_{s=1}^{k}\bigcup_{m_s=0}^{\tau_s-1}\tilde{\mathscr{P}}(s-1, H(s, m_s)), \tag{48}$$

where, for $1 \leqslant s \leqslant k$,

$$H(s, m_s) = 2^{-K(s-1)}M_s + m_s = \tau_k 2^{K(k-s)} + \tau_{k-1}2^{K(k-s-1)} + \ldots + \tau_{s+1}2^K + m_s.$$

Combining (18), (22), (43), (44) and (48), we have

$$\begin{aligned} D_K[\tilde{\mathcal{Q}}_M ; \mathcal{S}] &= \sum_{s=1}^{k} \sum_{m_s=0}^{\tau_s - 1} \tilde{D}_K(s-1, H(s, m_s)) \\ &= \sum_{s=1}^{k} \sum_{m_s=0}^{\tau_s - 1} \sum_{\mathbf{c} \in T(s-1, H(s,m_s))} \eta(s-1 ; \mathbf{c} ; H(s, m_s)). \end{aligned} \tag{49}$$

For $s = 1, \ldots, k$, let

$$X_s = \{\eta(s-1 ; \mathbf{c} ; H(s, m_s)) : 0 \leqslant m_s < \tau_s \text{ and } \mathbf{c} \in T(s-1, H(s, m_s))\},$$

and let $X = \bigcup_{s=1}^{k} X_s$. Then by (49), we have

$$\mathbb{E}(D_K[\tilde{\mathcal{Q}}_M ; \mathcal{S}])^2 = \sum_{\eta_1 \in X} \sum_{\eta_2 \in X} \mathbb{E}(\eta_1 \eta_2) = I_1 + 2I_2, \tag{50}$$

where

$$I_1 = \sum_{s=1}^{k} \sum_{\eta_1, \eta_2 \in X_s} \mathbb{E}(\eta_1 \eta_2) \quad \text{and} \quad I_2 = \sum_{1 \leqslant s < t \leqslant k} \sum_{\eta_1 \in X_s} \sum_{\eta_2 \in X_t} \mathbb{E}(\eta_1 \eta_2).$$

Consider first I_1. By (20) and Lemma 6, and noting that $|\eta| \leqslant 1$,

$$\begin{aligned} |I_1| &\leqslant \sum_{s=1}^{k} \sum_{m_s'=0}^{\tau_s - 1} \sum_{m_s''=0}^{\tau_s - 1} \#(T(s-1, H(s, m_s')) \cap T(s-1, H(s, m_s''))) \\ &\leqslant \sum_{s=1}^{k} \tau_s^2 2K 2^{(K-1)s} \leqslant K 2^{2K+2} 2^{(K-1)k} = K 2^{3K+1} 2^{(K-1)(k-1)} \\ &\leqslant K 2^{3K+1} M^{1-1/K}, \end{aligned} \tag{51}$$

in view of (47). We now consider I_2. Suppose that $1 \leqslant s < t \leqslant k$ and $\mathbf{c} \in T(t-1, H(t, m_t))$. Then there is at most one $\mathbf{c}' \in T(s-1, H(s, m_s))$ such that $C(s-1 ; \mathbf{c}') \cap C(t-1 ; \mathbf{c}) \neq \emptyset$. In fact, we then have $C(t-1 ; \mathbf{c}) \subset C(s-1 ; \mathbf{c}')$ and so

$$\frac{\mu_K(C(s-1 ; \mathbf{c}') \cap C(t-1 ; \mathbf{c}))}{\mu_K(C(s-1 ; \mathbf{c}'))} = 2^{K(s-t)}.$$

It follows from Lemma 6 and (20) that

$$\begin{aligned} |I_2| &\leqslant \sum_{t=1}^{k} \sum_{\eta \in X_t} \sum_{s=1}^{t-1} \sum_{m_s=0}^{\tau_s - 1} 2^{K(s-t)} \leqslant 2 \sum_{t=1}^{k} \sum_{\eta \in X_t} 1 \\ &= 2 \sum_{t=1}^{k} \sum_{m_t=0}^{\tau_t - 1} \#T(t-1, H(t, m_t)) \\ &\leqslant 4K \sum_{t=1}^{k} \sum_{m_t=0}^{\tau_t - 1} 2^{(K-1)(t-1)} \leqslant K 2^{K+2} \sum_{t=1}^{k} 2^{(K-1)(t-1)} \\ &\leqslant K 2^{K+3} 2^{(K-1)(k-1)} \leqslant K 2^{K+3} M^{1-1/K}, \end{aligned} \tag{52}$$

in view of (47). The lemma now follows on combining (50)–(52).

While Lemma 9 is sufficient to establish Theorem 3B in the case where $L = 1$, we need a stronger version of Lemma 9 if $L \geqslant 2$. For every natural number M and every residue class R of integers modulo q, let

$$\tilde{\mathcal{Q}}_M(R) = \{\tilde{\mathbf{q}}_n\colon\ 0 \leqslant n < m \text{ and } n \in R\}$$

and, for every compact and convex set $\mathcal{S} \subset U^K$, let

$$Z_K[\tilde{\mathcal{Q}}_M(R)\,;\,\mathcal{S}] = \#(\tilde{\mathcal{Q}}_M(R) \cap \mathcal{S}),$$

and write

$$D_K[\tilde{\mathcal{Q}}_M(R)\,;\,\mathcal{S}] = Z_K[\tilde{\mathcal{Q}}_M(R)\,;\,\mathcal{S}] - M'\mu_K(\mathcal{S}),$$

where $M' = \#\tilde{\mathcal{Q}}_M(R) = \#(R \cap [0, M))$.

LEMMA 10. *Let R be any residue class of integers modulo q, where q is odd. For every natural number M satisfying $1 \leqslant M \leqslant 2^{Kh}q$, we have*

$$\mathbb{E}(D_K[\tilde{\mathcal{Q}}_M(R)\,;\,\mathcal{S}])^2 \leqslant K2^{4K}(Mq^{-1} + 1)^{1-1/K}.$$

Proof. Let R be the residue class n_0 modulo q, where $0 \leqslant n_0 < q$. Then

$$\tilde{\mathcal{Q}}_M(R) = \{\tilde{\mathbf{q}}_{n_0+qn}\colon\ 0 \leqslant n < M'\},$$

where

$$M' \leqslant [(M - n_0)q^{-1}] + 1 \leqslant Mq^{-1} + 1. \tag{53}$$

In view of Lemma 4 and the independence between the randomization of F and the randomization of the points $\mathbf{q}(\mathbf{c})$, we have

$$\mathbb{E}(D_K[\tilde{\mathcal{Q}}_M(R)\,;\,\mathcal{S}])^2 = \mathbb{E}(D_K[\tilde{\mathcal{Q}}_M\,;\,\mathcal{S}])^2. \tag{54}$$

The result now follows on combining (53), (54) and Lemma 9.

7. *The van der Corput–Halton–Hammersley sequence*

Let p_j be the jth odd prime. For any integer n satisfying $0 \leqslant n < p_j^h$, write

$$n = \sigma_{h,j}p_j^{h-1} + \sigma_{h-1,j}p_j^{h-2} + \ldots + \sigma_{1,j},$$

where $\sigma_{1,j}, \ldots, \sigma_{h,j} \in \{0, 1, \ldots, p_j - 1\}$, and let

$$y_j(n) = \sigma_{1,j}p_j^{-1} + \ldots + \sigma_{h,j}p_j^{-h} = p_j^{-h}(\sigma_{1,j}p_j^{h-1} + \sigma_{2,j}p_j^{h-2} + \ldots + \sigma_{h,j}).$$

We extend the range of definition of $y_j(n)$ over th set $\mathbb{Z}$ by periodicity so as to ensure that $y_j(n + p_j^h) = y_j(n)$ for every integer n. Then it is very easy to see that

LEMMA 11. *Let $s_j \in \{0, 1, \ldots, h\}$. If $b_j \in \mathbb{Z}$ and $I(p_j, s_j, b_j) \subset U$, then*

$$\{n \in \mathbb{Z}\colon\ y_j(n) \in I(p_j, s_j, b_j)\}$$

is a residue class modulo $p_j^{s_j}$.

Let $p_1, \ldots, p_L$ be the first L odd primes, and let

$$\mathbf{y}_n = (y_1(n), \ldots, y_L(n))$$

for every $n \in \mathbb{Z}$. Then it follows from Lemma 11 and the Chinese remainder

theorem that

LEMMA 12. *Let* $s_1, \ldots, s_L \in \{0, 1, \ldots, h\}$. *If* $b_1, \ldots, b_L \in \mathbb{Z}$ *and*

$$I(p_1, s_1, b_1) \times \ldots \times I(p_L, s_L, b_L) \subset U^L,$$

then

$$\{n \in \mathbb{Z}: \mathbf{y}_n \in I(p_1, s_1, b_1) \times \ldots \times I(p_L, s_L, b_L)\}$$

is a residue class modulo $p_1^{s_1} \ldots p_L^{s_L}$.

The van der Corput–Halton–Hammersley sequence $\mathbf{y}_n$ has been used on many occasions to give upper bound results in irregularities of distribution (see Halton [7], Hammersley [8], Roth [11] and Chen [4]).

8. *Modification of the van der Corput–Halton–Hammersley sequence*

We denote by $\mathcal{M}_{h,L}$ the set of all matrices $S = (\beta_{t,j})$ with integer entries $\beta_{t,j}$ satisfying $0 \leqslant \beta_{t,j} < p_j$ for each $j = 1, \ldots, L$ and $t = 1, \ldots, h$. It is clear that $\mathcal{M}_{h,L}$ has $(p_1 \ldots p_L)^h$ elements.

Let $S \in \mathcal{M}_{h,L}$. We construct a modified sequence $\mathbf{y}_n(S)$ as follows. Suppose that $0 \leqslant n < p_j^h$ and

$$y_j(n) = \sigma_{1,j} p_j^{-1} + \ldots + \sigma_{h,j} p_j^{-h}.$$

For $t = 1, \ldots, h$, let $\sigma_{t,j}^S$ be defined by

$$0 \leqslant \sigma_{t,j}^S < p_j \quad \text{and} \quad \sigma_{t,j}^S \equiv \sigma_{t,j} + \beta_{t,j} \pmod{p_j},$$

and let

$$y_j^S(n) = \sigma_{1,j}^S p_j^{-1} + \ldots + \sigma_{h,j}^S p_j^{-h}.$$

Then clearly $y_j^S(n) \in U$. Again, we extend the range of definition of $y_j^S(n)$ over the set $\mathbb{Z}$ by periodicity so as to ensure that $y_j^S(n + p_j^h) = y_j^S(n)$ for every integer n. We then define

$$\mathbf{y}_n(S) = (y_1^S(n), \ldots, y_L^S(n)).$$

It is not difficult to prove

LEMMA 13. *Let* $S \in \mathcal{M}_{h,L}$, *and let* $s_1, \ldots, s_L \in \{0, 1, \ldots, h\}$. *If* $b_1, \ldots, b_L \in \mathbb{Z}$ *and* $I(p_1, s_1, b_1) \times \ldots \times I(p_L, s_L, b_L) \subset U^L$, *then*

$$\{n \in \mathbb{Z}: \mathbf{y}_n^S \in I(p_1, s_1, b_1) \times \ldots \times I(p_L, s_L, b_L)\}$$

is a residue class modulo $p_1^{s_1} \ldots p_L^{s_L}$.

9. *The sequence: randomized and modified*

We now summarize our argument so far. For every non-negative integer n, let $\mathbf{p}_n = (\mathbf{q}_n, \mathbf{y}_n) \in U^{K+L}$, where $\mathbf{q}_n \in U^K$ is defined in § 4 and where $\mathbf{y}_n \in U^L$ is defined in § 7. We randomize the sequence $\mathbf{q}_n$ in § 5 to obtain the sequence $\tilde{\mathbf{q}}_n$ and modify the sequence $\mathbf{y}_n$ in § 8 to obtain $\mathbf{y}_n(S)$. Combining these, we obtain the randomized and modified version of $\mathbf{p}_n$, namely

$$\tilde{\mathbf{p}}_n(S) = (\tilde{\mathbf{q}}_n, \mathbf{y}_n(S)). \tag{55}$$

Note that the sequence $\tilde{\mathbf{q}}_n$ satisfies Lemma 10 and that the sequence $\mathbf{y}_n(S)$ satisfies Lemma 13. We shall combine these in the next section.

We shall write

$$\tilde{\mathcal{P}}_M = \{\tilde{\mathbf{p}}_0, \ldots, \tilde{\mathbf{p}}_{M-1}\} \tag{56}$$

and

$$\tilde{\mathcal{P}}_M(S) = \{\tilde{\mathbf{p}}_0(S), \ldots, \tilde{\mathbf{p}}_{M-1}(S)\}. \tag{57}$$

10. *Subdivision of the rectangular box*

In this section, we follow a combination of arguments of Roth [**11**] and Chen [**5**]. Let

$$B^* = [0, \eta_1) \times \ldots \times [0, \eta_L) \in U^L, \tag{58}$$

where, for every $j = 1, \ldots, L$, the number η_j is an integer multiple of p_j^{-h}. For $j = 1, \ldots, L$ and $s = 1, \ldots, h$, let $\xi_{s,j}$ denote the greatest integer multiple of p_j^{-s} not exceeding η_j, and let

$$J_{s,j} = [\xi_{s-1,j}, \xi_{s,j}),$$

with the convention that $\xi_{0,j} = 0$. Then for $j = 1, \ldots, L$,

$$[0, \eta_j] = \bigcup_{s=1}^{h} J_{s,j},$$

so that

$$B^* = \bigcup_{s_1=1}^{h} \ldots \bigcup_{s_L=1}^{h} (J_{s_1,1} \times \ldots \times J_{s_L,L}). \tag{59}$$

Consider now the distribution $\tilde{\mathcal{P}}_M$ of M points in U^{K+L} given by (56). For any sets $\mathcal{S} \subset U^K$ and $\mathcal{B} \subset U^L$, let

$$D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times \mathcal{B}] = \#(\tilde{\mathcal{P}}_M \cap (\mathcal{S} \times \mathcal{B})) - M\mu_K(\mathcal{S})\mu_L(\mathcal{B}).$$

Then it follows from (59) that for every set $\mathcal{S}$ in U^K,

$$D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times B^*] = \sum_{s_1=1}^{h} \ldots \sum_{s_L=1}^{h} D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times J_{s_1,1} \times \ldots \times J_{s_L,L}],$$

so that

$$|D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times B^*]|^2 = \sum_{s_1'=1}^{h} \ldots \sum_{s_L'=1}^{h} \sum_{s_1''=1}^{h} \ldots \sum_{s_L''=1}^{h} D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times J_{s_1',1} \times \ldots \times J_{s_L',L}] \times D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times J_{s_1'',1} \times \ldots \times J_{s_L'',L}]. \tag{60}$$

Note that for every $j = 1, \ldots, L$ and $s = 1, \ldots, h$,

$$J_{s,j} = \bigcup_{\alpha=1}^{\nu_{s,j}} J_{s,j,\alpha} \tag{61}$$

where

$$\nu_{s,j} = p_j^s(\xi_{s,j} - \xi_{s-1,j})$$

and, for every $\alpha = 1, \ldots, \nu_{s,j}$, the interval $J_{s,j,\alpha}$ is of the type $I(p_j, s, c)$ where $c \in \mathbb{Z}$. Note also that

$$0 \leqslant \nu_{s,j} \leqslant p_j. \tag{62}$$

If we write $\mathbf{s} = (s_1, \ldots, s_L)$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_L)$, and let

$$D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}) = D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times J_{s_1,1} \times \ldots \times J_{s_L,L}]$$

and

$$D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}, \boldsymbol{\alpha}) = D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times J_{s_1,1,\alpha_1} \times \ldots \times J_{s_L,L,\alpha_L}],$$

then it follows from (60) and (61) that

$$|D[\tilde{\mathcal{P}}_M ; \mathcal{S} \times B^*]|^2 = \sum_{s'_1=1}^{h} \dots \sum_{s'_L=1}^{h} \sum_{s''_1=1}^{h} \dots \sum_{s''_L=1}^{h} D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}')D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}'') \quad (63)$$

and

$$D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}')D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}'') = \sum_{\alpha'_1=1}^{\nu_{s'_1,1}} \dots \sum_{\alpha'_L=1}^{\nu_{s'_L,L}} \sum_{\alpha''_1=1}^{\nu_{s''_1,1}} \dots \sum_{\alpha''_L=1}^{\nu_{s''_L,L}} D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}', \boldsymbol{\alpha}')D(\tilde{\mathcal{P}}_M ; \mathcal{S} ; \mathbf{s}'', \boldsymbol{\alpha}''). \quad (64)$$

LEMMA 14. *For every* $\mathbf{s}', \mathbf{s}'' \in \{1, \dots, h\}^L$, *for every* $\alpha'_j = 1, \dots, \nu_{s'_j,j}$ *and for every* $\alpha''_j = 1, \dots, \nu_{s''_j,j}$, *let*

$$m_j = \min\{s'_j, s''_j\} \quad \text{and} \quad d_j = |s'_j - s''_j|,$$

and let $J^*_{s'_j,j,\alpha'_j}$ *and* $J^*_{s''_j,j,\alpha''_j}$ *denote the intervals of the form* $I(p_j, m_j, c)$ *containing* $J_{s'_j,j,\alpha'_j}$ *and* $J_{s''_j,j,\alpha''_j}$ *respectively. Then*

$$\sum_{S \in \mathcal{M}_{h,L}} D(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}', \boldsymbol{\alpha}')D(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}'', \boldsymbol{\alpha}'') = p_1^{-d_1} \dots p_L^{-d_L} \sum_{S \in \mathcal{M}_{h,L}} D^*(\tilde{P}_M(S) ; \mathcal{S} ; \mathbf{s}', \boldsymbol{\alpha}')D^*(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}'', \boldsymbol{\alpha}''), \quad (65)$$

where

$$D^*(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}', \boldsymbol{\alpha}') = D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J^*_{s'_1,1,\alpha'_1} \times \dots \times J^*_{s'_L,L,\alpha'_L}] \quad (66)$$

and

$$D^*(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}'', \boldsymbol{\alpha}'') = D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J^*_{s''_1,1,\alpha''_1} \times \dots \times J^*_{s''_L,L,\alpha''_L}]. \quad (67)$$

Proof. We shall only show that

$$\sum_{S \in \mathcal{M}_{h,L}} D(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}', \boldsymbol{\alpha}')D(\tilde{\mathcal{P}}_M(S) ; \mathcal{S} ; \mathbf{s}'', \boldsymbol{\alpha}'') = p_1^{-d_1} \sum_{S \in \mathcal{M}_{h,L}} D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J^*_{s'_1,1,\alpha'_1} \times J']D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J^*_{s''_1,1,\alpha''_1} \times J''], \quad (68)$$

where

$$J' = J_{s'_2,2,\alpha'_2} \times \dots \times J_{s'_L,L,\alpha'_L} \quad \text{and} \quad J'' = J_{s''_2,2,\alpha''_2} \times \dots \times J_{s''_L,L,\alpha''_L}.$$

Equation (65) then follows if we repeat the argument $(L-1)$ times. To prove (68), we may assume, without loss of generality, that $s'_1 \leqslant s''_1$, so that $m_1 = s'_1$. Let $S = (\beta_{t,j})$. Then the term

$$D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J_{s'_1,1,\alpha'_1} \times J'] = D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J^*_{s'_1,1,\alpha'_1} \times J']$$

is independent of the entries $\beta_{s'+1,1}, \beta_{s'+2,1}, \dots, \beta_{h,1}$ of S, while the term

$$D[\tilde{\mathcal{P}}_M(S) ; \mathcal{S} \times J_{s''_1,1,\alpha''_1} \times J'']$$

is independent of the entries $\beta_{s''+1,1}, \beta_{s''+2,1}, \dots, \beta_{h,1}$ of S. Furthermore, if all entries $\beta_{t,j}$ of the matrix S are fixed except for

$$\beta_{s'+1,1}, \beta_{s'+2,1}, \dots, \beta_{s'',1}, \quad (69)$$

then

$$\sum_{\beta_{s'+1,1}=0}^{p_1-1} \sum_{\beta_{s'+2,1}=0}^{p_1-1} \dots \sum_{\beta_{s'',1}=0}^{p_1-1} D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J_{s''_1,1,\alpha''_1}\times J''] = D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s''_1,1,\alpha''_1}\times J''], \quad (70)$$

and note that the right-hand side of (70) is independent of the entries (69). It follows that if all entries $\beta_{t,j}$ of the matrix S are fixed except for (69), then

$$\sum_{\beta_{s'+1,1}=0}^{p_1-1} \sum_{\beta_{s'+2,1}=0}^{p_1-1} \dots \sum_{\beta_{s'',1}=0}^{p_1-1} D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J_{s'_1,1,\alpha'_1}\times J']D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J_{s''_1,1,\alpha''_1}\times J''] = D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s'_1,1,\alpha'_1}\times J']D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s''_1,1,\alpha''_1}\times J'']. \quad (71)$$

Summing (71) over all entries $\beta_{t,j}$ of S apart from (69), we have

$$\begin{aligned}\sum_{S\in\mathcal{M}_{h,L}} & D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J_{s'_1,1,\alpha'_1}\times J']D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J_{s''_1,1,\alpha''_1}\times J''] \\ &= \sum_{S\in\mathcal{M}^*_{h,L}} D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s'_1,1,\alpha'_1}\times J']D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s''_1,1,\alpha''_1}\times J''] \\ &= p_1^{-d_1}\sum_{S\in\mathcal{M}_{h,L}} D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s'_1,1,\alpha'_1}\times J']D[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times J^*_{s''_1,1,\alpha''_1}\times J''],\end{aligned}$$

where $\mathcal{M}^*_{h,L} = \{S\in\mathcal{M}_{h,L}\colon \beta_{s'+1,1}=\beta_{s'+2,1}=\dots=\beta_{s'',1}=0\}$ has $p_1^{-d_1}(p_1\dots p_L)^h$ elements.

11. *Completion of the proof*

We now examine the set $\tilde{\mathcal{P}}_M(S)$ more closely. By (55) and (57),

$$\tilde{\mathcal{P}}_M(S) = \{(\tilde{\mathbf{q}}_0, \mathbf{y}_0(S)), \dots, (\tilde{\mathbf{q}}_{M-1}, \mathbf{y}_{M-1}(S))\}.$$

Clearly if $\mathcal{S}\subset U^K$ and $\mathcal{B}\subset U^L$, then $(\tilde{\mathbf{q}}_n, \mathbf{y}_n(S))\in\mathcal{S}\times\mathcal{B}$ if and only if $\tilde{\mathbf{q}}_n\in\mathcal{S}$ and $\mathbf{y}_n(S)\in\mathcal{B}$. Suppose now that

$$\mathcal{B} = I(p_1, m_1, c_1)\times\dots\times I(p_L, m_L, c_L).$$

Then $\mathbf{y}_n(S)\in\mathcal{B}$ if and only if n belongs to a residue class modulo $p_1^{m_1}\dots p_L^{m_L}$, by Lemma 13.

It now follows that there exist residue classes R' and R'' modulo $p_1^{m_1}\dots p_L^{m_L}$, depending only on $\mathbf{s}'$, $\mathbf{s}''$, $\boldsymbol{\alpha}'$, $\boldsymbol{\alpha}''$ and S, such that the terms (66) and (67) can be represented respectively in the form

$$D^*(\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\,;\,\mathbf{s}',\boldsymbol{\alpha}') = D_K[\tilde{\mathcal{Q}}_M(R')\,;\,\mathcal{S}] \quad (72)$$

and

$$D^*(\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\,;\,\mathbf{s}'',\boldsymbol{\alpha}'') = D_K[\tilde{\mathcal{Q}}_M(R'')\,;\,\mathcal{S}]. \quad (73)$$

Hence by Lemma 10, for every compact and convex $\mathcal{S}\subset U^K$, we have

$$\begin{aligned}\mathbb{E}(D^*(\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\,;\,\mathbf{s}',\boldsymbol{\alpha}')&D^*(\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\,;\,\mathbf{s}'',\boldsymbol{\alpha}'')) \\ &\leqslant (\mathbb{E}(D^*(\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\,;\,\mathbf{s}',\boldsymbol{\alpha}'))^2\mathbb{E}(D^*(\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\,;\,\mathbf{s}'',\boldsymbol{\alpha}''))^2)^{\frac{1}{2}} \\ &\leqslant K2^{4K}(Mp_1^{-m_1}\dots p_L^{-m_L}+1)^{1-1/K}. \quad (74)\end{aligned}$$

Combining (63)–(65), Lemma 14 and (74), we have, for every compact and

convex $\mathscr{S} \subset U^K$ and every B^* of the form (58), that

$$\mathbb{E}\Big(\sum_{S \in \mathscr{M}_{h,L}} |D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B^*]|^2\Big) \leqslant K 2^{4K} \sum_{S \in \mathscr{M}_{h,L}} \sum^* p_1^{-d_1} \dots p_L^{-d_L} (M p_1^{-m_1} \dots p_L^{-m_L} + 1)^{1-1/K}, \quad (75)$$

where

$$\sum^* = \sum_{s_1'=1}^{h} \dots \sum_{s_L'=1}^{h} \sum_{s_1''=1}^{h} \dots \sum_{s_L''=1}^{h} \sum_{\alpha_1'=1}^{\nu_{s_1',1}} \dots \sum_{\alpha_L'=1}^{\nu_{s_L',L}} \sum_{\alpha_1''=1}^{\nu_{s_1'',1}} \dots \sum_{\alpha_L''=1}^{\nu_{s_L'',L}} \quad (76)$$

and where m_j and d_j are defined in Lemma 14. Since the summand on the right-hand side of (75) is independent of $\boldsymbol{\alpha}'$ and $\boldsymbol{\alpha}''$, it follows from (62) that

$$\mathbb{E}\Big(\sum_{S \in \mathscr{M}_{h,L}} |D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B^*]|^2\Big) \ll_{K,L} \sum_{S \in \mathscr{M}_{h,L}} M^{1-1/K} (p_1 \dots p_L)^2 \Sigma_1 \dots \Sigma_L,$$

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

$$\Sigma_j = \sum_{s_j'=1}^{h} \sum_{s_j''=1}^{h} p_j^{-d_j} p_j^{-(1-1/K)m_j} \leqslant 2 \sum_{s=1}^{h} p_j^{-(1-1/K)s} \sum_{t=0}^{\infty} p_j^{-t} \ll_{K,j} 1.$$

Hence

$$\mathbb{E}\Big(\sum_{S \in \mathscr{M}_{h,L}} |D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B^*]|^2\Big) \leqslant C(K, L)(p_1 \dots p_L)^h M^{1-1/K}, \quad (77)$$

where $C(K, L)$ is a constant depending only on K and L.

Suppose now that $\mathbf{y} = (y_1, \dots, y_L) \in U^L$. Let $\eta_j = \eta_j(y_j) = -p_j^{-h}[-p_j^h y_j]$; *i.e.* let η_j be the least integer multiple of p_j^{-h} not less than y_j. Let $\boldsymbol{\eta} = (\eta_1, \dots, \eta_L)$. Writing $h = [\log_2 N] + 1$, we clearly have

$$N \leqslant p_j^h \quad (78)$$

for every $j = 1, \dots, L$.

LEMMA 15. *For every $\mathscr{S} \subset U^K$, for every $S \subset \mathscr{M}_{h,L}$ and for every natural number $M \leqslant N$, we have*

$$|D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B(\mathbf{y})] - D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B(\boldsymbol{\eta})]| \leqslant L. \quad (79)$$

Proof. For $j = 0, \dots, L$ and for any fixed $\mathbf{y} \in U^L$, let

$$B^{(j)} = B^{(j)}(\mathbf{y}) = [0, \eta_1) \times \dots \times [0, \eta_j) \times [0, y_{j+1}) \times \dots \times [0, y_L). \quad (80)$$

Then clearly $B^{(0)} = B(\mathbf{y})$ and $B^{(L)} = B(\boldsymbol{\eta})$. To prove (79), it suffices to prove that for every $j = 1, \dots, L$,

$$|D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B^{(j)}] - D[\tilde{\mathscr{P}}_M(S); \mathscr{S} \times B^{(j-1)}]| \leqslant 1. \quad (81)$$

Clearly it follows from (78) and (80) that

$$\begin{aligned} 0 &\leqslant \mu(\mathscr{S} \times B^{(j)}) - \mu(\mathscr{S} \times B^{(j-1)}) \\ &= \mu_K(\mathscr{S}) \mu_L(B^{(j)} \setminus B^{(j-1)}) \\ &\leqslant \mu_L(B^{(j)} \setminus B^{(j-1)}) \leqslant p_j^{-h} \leqslant N^{-1}, \end{aligned}$$

so that

$$M\mu(\mathscr{S} \times B^{(j)}) - M\mu(\mathscr{S} \times B^{(j-1)}) \leqslant 1.$$

To prove (81), it remains to show that

$$0 \leqslant Z[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times B^{(j)}] - Z[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times B^{(j-1)}] \leqslant 1.$$

The first inequality is obvious, since $B^{(j-1)} \subset B^{(j)}$. On the other hand,

$$B^{(j)} \setminus B^{(j-1)} \subset [0,1)^{j-1} \times I(p_j, h, c_j) \times [0,1)^{L-j}$$

for some interval $I(p_j, h, c_j) \subset [0,1)$, so that

$$\begin{aligned} Z[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times B^{(j)}] &- Z[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times B^{(j-1)}] \\ &\leqslant Z[\tilde{\mathcal{P}}_M(S)\,;\,\mathcal{S}\times (B^{(j)}\setminus B^{(j-1)})] \\ &\leqslant Z_L[\{\mathbf{y}_0(S), \ldots, \mathbf{y}_{M-1}(S)\}\,;\,[0,1)^j \times I(p_j, h, c_j) \times [0,1)^{L-j}] \leqslant 1, \end{aligned}$$

in view of Lemma 13, (78) and the restriction $M \leqslant N$.

It now follows from (77) and Lemma 15 that

$$\sum_{S\in\mathcal{M}_{h,L}} \mathbb{E}\Big(\frac{1}{N}\sum_{M=1}^{N}\int_0\int_{\mathcal{S}}\int_{U^K}\int_{U^L} |D[\tilde{\mathcal{P}}_M(S)\,;A(\lambda,\tau,\mathbf{u})\times B(\mathbf{y})]|^2\,d\mathbf{y}\,d\mathbf{u}\,d\tau\,d\lambda\Big) \ll_{A,L} (p_1\ldots p_L)^h N^{1-1/K}.$$

Inequality (1) follows immediately on noting that $\mathcal{M}_{h,L}$ has precisely $(p_1 \ldots p_L)^h$ elements.

References

1. J. BECK, 'Irregularities of distribution I', *Acta Math.* 159 (1987) 1–49.
2. J. BECK and W. W. L. CHEN, 'Note on irregularities of distribution', *Mathematika* 33 (1986) 148–163.
3. J. BECK and W. W. L. CHEN, *Irregularities of distribution*, Cambridge Tracts in Mathematics 89 (Cambridge University Press, 1987).
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* (2) 34 (1983) 257–279.
6. K. L. CHUNG, *A course in probability theory* (Academic Press, New York, 1974).
7. J. H. HALTON, 'On the efficiency of certain quasirandom sequences of points in evaluating multidimensional integrals', *Numer. Math.* 2 (1960) 84–90.
8. J. M. HAMMERSLEY, 'Monte Carlo methods for solving multivariable problems', *Ann. New York Acad. Sci.* 86 (1960) 844–874.
9. H. L. MONTGOMERY, 'Irregularities of distribution by means of power sums', preprint, University of Michigan, 1984.
10. K. F. ROTH, 'On irregularities of distribution', *Mathematika* 1 (1954) 73–79.
11. K. F. ROTH, 'On irregularities of distribution IV', *Acta Arith.* 37 (1980) 67–75.
12. W. M. SCHMIDT, *Lectures on irregularities of distribution* (Tata Institute of Fundamental Research, Bombay, 1977).

Department of Mathematics
Rutgers University
New Brunswick
New Jersey 08903
U.S.A.

Department of Mathematics
Imperial College
Huxley Building
180 *Queen's Gate*
London SW7 2BZ